CLOUD<br>ACCOUNTABILITY<br>PROJECT

# D:B-2.4 Requirements Report

| | |
|---|---|
| **Deliverable Number** | D22.4 |
| **Work Package** | WP 22 |
| **Version** | Final |
| **Deliverable Lead Organisation** | SINTEF |
| **Dissemination Level** | PU |
| **Contractual Date of Delivery (release)** | 30/09/2014 |
| **Date of Delivery** | 14/11/2014 |

**Editors**

Daniela S. Cruzes (SINTEF)
Martin Gilje Jaatun (SINTEF)

**Contributors**

Martin Gilje Jaatun (SINTEF), Daniela Soares Cruzes (SINTEF), Massimo Felici (HP), Børge Haugset (SINTEF), Karin Bernsmed (SINTEF), Carmen Fernandez Gago (UMA), Chris Reed (QMUL) , Ronald Leenes (TiU)

**Reviewers**

Fredric Gittler (HP), Vasilis Tountopoulos (HTC)

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

FP7-ICT-2011-8-317550-A4CLOUD

SEVENTH FRAMEWORK PROGRAMME

## Executive Summary

The Cloud Accountability project (A4Cloud) is working towards an accountability-based approach, which enables and utilises different mechanisms and tools that help cloud customers and providers as well as regulators and auditors to make sure that the obligations to protect personal data and business confidential data are adhered to. The over-arching goal of the elicitation work package WP 22 is to ensure that the needs of stakeholders are heard within the project, by gathering requirements.

The Description of Work (DoW) outlines that WP 22 is to accomplish its goal through a set of stakeholder workshops. WP 22 has therefore organised four different stakeholder workshops.

1. The first workshop (WS1) discussed with stakeholders the notion of accountability and dealt with eliciting the initial accountability requirements in the A4Cloud project. It also provided a means for refining the three selected business use cases we had thought out in the project.
2. The second workshop (WS2) dealt with risk perception. The aim was to focus on the notion of risk and trust assessment of cloud services, future Internet services and dynamic combinations of such services (mashups). The workshop focused on how emerging threats in the cloud are perceived by stakeholders. Moreover, it analysed emerging relationships between accountability, risk and trust.
3. The third workshop (WS3) presented stakeholders with accountability mechanisms (in particular, software tools developed by A4Cloud) in order to gather their operational experiences and expectations about accountability in the cloud. WS3 consisted of different sub-workshops tailored to specific cloud actors, in particular, individual cloud customers and cloud providers.
4. The fourth workshop (WS4) covered aspects not previously touched upon in the other workshops, exposing stakeholders to metrics for accountability and incident response management in a cloud computing setting. Furthermore, a small number of external legal experts provided input on high-level descriptions of tools developed in the project.

Many project partners took part in hosting and participating at the different workshops, providing insights from the various domains of knowledge these institutions hold and the types of stakeholders they attract. The previous three deliverables that have been produced by WP 22 contain results from the first three stakeholder elicitation workshops. In total, the elicitation effort of the A4Cloud project has involved more than 300 stakeholders who contributed to the identification of detailed accountability requirements. This has allowed the project to gather requirements from different stakeholders, ranging from individual cloud customers to organisational cloud customers and cloud providers. The requirements elicitation workshops highlighted how stakeholders understand accountability and what their priorities and concerns are about data protection in the cloud.

In addition to the stakeholder requirements, the A4Cloud project has devised an expert-driven set of high-level requirements which, from an organisational perspective, set out what it takes to be an accountable organisation. These requirements are intended to supplement the requirements elicitation process described in the DoW by providing a set of expert-driven high-level *guiding-light requirements*, formulated as requirements that accountable organisations should meet in a cloud ecosystem. In short, these requirements state that an accountable organisation that processes personal and/or business confidential data must:

1. *demonstrate willingness and capacity to be responsible and answerable for its data practices*
2. *define policies regarding their data practices*
3. *monitor their data practices*
4. *correct policy violations, and*
5. *demonstrate policy compliance.*

These guiding light requirements have informed other work packages too. On the one hand, they are aligned with the conceptual framework of accountability (as defined by WP 32). On the other hand, they provide a means for communicating accountability requirements at the organisational level, and hence inform accountability practices.

In order to support the elicitation and analysis of requirements, WP 22 has also created and maintained a central requirement repository for all the requirements that have been collected in the project, ensuring full traceability for future use (that is, supporting best practices in requirements engineering). This repository consists of the requirements elicited by the four elicitation workshops together with other technical requirements that have originated from the conceptual analyses and technical contributions conducted by the other work packages in the project. The requirements gathered have been classified in terms of accountability attributes (identified in the WP 32 accountability model) and cloud actors. The classification in terms of accountability attributes and cloud actors supported the initial consolidation of requirements and the alignment with the accountability conceptual framework. The gathered accountability requirements bridge from conceptual aspects of accountability to operational objectives of accountability. Grouping and analysing them highlights specific functional requirements that are directly related to the actors involved in the cloud service delivery chain, and also requirements for accountability mechanisms that are related to the tools and technologies being developed in the project. An initial analysis and refinement of these requirements shows that most requirements target cloud providers and many of them are related to transparency. In addition there is a strong focus on evidence. Other requirements are related to incident management, security mechanisms, data governance, data protection legislation, policies and audits. Finally, some requirements are concerned with specific accountability mechanisms (in particular, software tools) – Cloud Offerings Advisory Tool (COAT), Data Track Tool and Accountability Policy Language (A-PPL) – which have been used as an elicitation means with stakeholders (in particular, during WS3) and have been developed by the A4Cloud project. The COAT and Data Track Tool were chosen due to the fact that they were the most advanced (in terms of development status) at the time of the workshops.

This deliverable is a consolidated report of all requirements that have been elicited during the first two years of the project. In addition, it includes results from WS4, as well as the guiding lights requirements and a description of the dissemination activities that have been performed in the work package. To summarise, WP 22 has produced four reports and maintained the requirements in the repository. In addition a number of additional activities have been organised that support the overall goal. On a wider scale, WP 22 has contributed to project dissemination through participation in workshops, presentation events and social media channels, and has also provided a venue for exposing early results from the project to stakeholders, collecting their feedback, and enabling necessary course adjustments in the research process. For some accountability mechanisms, stakeholder feedback was especially helpful (to the work packages developing the tools) in order to externalise the requirements for the specific software tools, since such requirements capture stakeholder expectations about novel accountability mechanisms.

Beside gathering stakeholder requirements, the main contribution of WP 22 in A4Cloud was to guide and inform project work packages (and their tasks), making sure they reflected the needs of stakeholders. Through communication with different stakeholders (e.g. individual cloud customers, cloud providers), WP 22 has provided other work packages with stakeholder requirements reflecting the stakeholders' understanding of accountability. These requirements inform the development of the A4Cloud toolset and the demonstrator, which will be used as a means to operationally validate the A4Cloud accountability-based approach (as well as to further consolidate the accountability requirements) and to communicate the project results to stakeholders. In addition, we foresee that the consolidated accountability requirements to be useful for various stakeholders, e.g. cloud, security and privacy research communities as well as cloud and information technology providers (the ICT industry), who are developing software and services to be deployed in public and private cloud ecosystems.

## Table of Contents

## Index of Figures

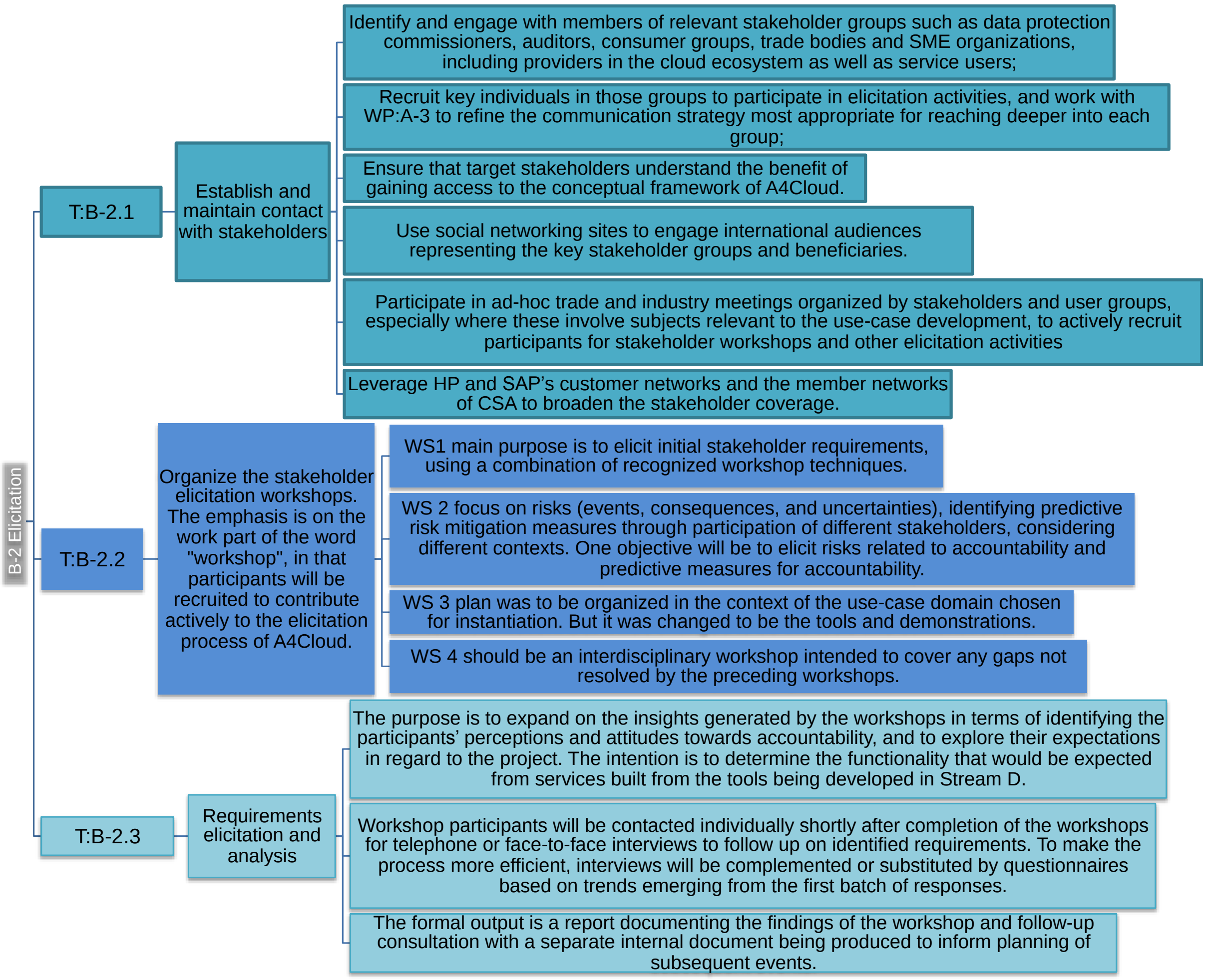
## Index of Tables

# 1 Introduction

The overall goal of WP 22 Elicitation has been to bring relevant stakeholder perceptions of accountability issues into the A4Cloud project. By engaging with a broad spectrum of stakeholders, and making use of them in various requirement elicitation activities, we were able to provide insights influencing the project's understanding of accountability.

## 1.1 Requirements Elicitation Process

The requirements elicitation process described in the DoW (as shown in Figure 1) is based on obtaining requirements from the stakeholders and ensuring that the project results meet the actual needs of the various stakeholders. The DoW defines the role of accountability in the emerging information society as an important pre-requisite for trust in online services. The objective of WP 22 is also to ensure that project activities reflect the needs of stakeholder groups' specific goals. In that direction, in the activities performed for this work package, we focused on engagement with a broad base of relevant stakeholders for elicitation purposes using different methodologies to elicit, refine and validate the requirements for the project, as will be described in this document. We also sought to externalise the tacit understanding that the A4Cloud project partners have through describing a set of guiding lights – high-level organisational requirements. Section 1.1 explains how we addressed these goals.


B-2 Elicitation
T:B-2.1
Establish and maintain contact with stakeholders
T:B-2.2
T:B-2.3
Requirements elicitation and analysis

Identify and engage with members of relevant stakeholder groups such as data protection commissioners, auditors, consumer groups, trade bodies and SME organizations, including providers in the cloud ecosystem as well as service users;

Recruit key individuals in those groups to participate in elicitation activities, and work with WP:A-3 to refine the communication strategy most appropriate for reaching deeper into each group;

Ensure that target stakeholders understand the benefit of gaining access to the conceptual framework of A4Cloud.

Use social networking sites to engage international audiences representing the key stakeholder groups and beneficiaries.

Participate in ad-hoc trade and industry meetings organized by stakeholders and user groups, especially where these involve subjects relevant to the use-case development, to actively recruit participants for stakeholder workshops and other elicitation activities

Leverage HP and SAP's customer networks and the member networks of CSA to broaden the stakeholder coverage.

Organize the stakeholder elicitation workshops. The emphasis is on the work part of the word "workshop", in that participants will be recruited to contribute actively to the elicitation process of A4Cloud.

WS1 main purpose is to elicit initial stakeholder requirements, using a combination of recognized workshop techniques.

WS 2 focus on risks (events, consequences, and uncertainties), identifying predictive risk mitigation measures through participation of different stakeholders, considering different contexts. One objective will be to elicit risks related to accountability and predictive measures for accountability.

WS 3 plan was to be organized in the context of the use-case domain chosen for instantiation. But it was changed to be the tools and demonstrations.

WS 4 should be an interdisciplinary workshop intended to cover any gaps not resolved by the preceding workshops.

The purpose is to expand on the insights generated by the workshops in terms of identifying the participants' perceptions and attitudes towards accountability, and to explore their expectations in regard to the project. The intention is to determine the functionality that would be expected from services built from the tools being developed in Stream D.

Workshop participants will be contacted individually shortly after completion of the workshops for telephone or face-to-face interviews to follow up on identified requirements. To make the process more efficient, interviews will be complemented or substituted by questionnaires based on trends emerging from the first batch of responses.

The formal output is a report documenting the findings of the workshop and follow-up consultation with a separate internal document being produced to inform planning of subsequent events.

**Figure 1: Tasks in the WP 22 Elicitation work package.**

## 1.2 Methodology for Reflecting the Needs of Stakeholder Groups

The primary measure of success of a software system is the degree to which it meets the purpose for which it was intended [6]. In A4Cloud the WP 22 elicitation work package plays an important role on achieving this goal. Broadly speaking, requirements engineering (RE) is the process of discovering that purpose, by identifying stakeholders and their needs, and documenting these in a form that is amenable to analysis, communication, and subsequent implementation. There are a number of inherent difficulties in this process [1][2]; stakeholders may be numerous and distributed (as it is the case in A4Cloud). In A4Cloud, a *stakeholder* means a person, group or organisation that affects or can be affected by the A4Cloud project results [3]. Another challenge is that the stakeholders' goals may vary and conflict, depending on their perspectives of the environment in which they work and the tasks they wish to accomplish. Finally, the stakeholders' goals may not be explicit or may be difficult to articulate, and, inevitably, satisfaction of these goals may be constrained by a variety of factors outside their control. For addressing these challenges we have used different approaches to elicit requirements in WP 22. The aim of involving stakeholders in workshops is to gather a broad spectrum of requirements, good practices and risks related to the cloud eco-system covering the diverse range of geographical (including legal) constraints and challenges, sector/industry-specific requirements and cloud models. As planned in the DoW, four stakeholder elicitation workshops were performed in the A4Cloud project (see Figure 2).

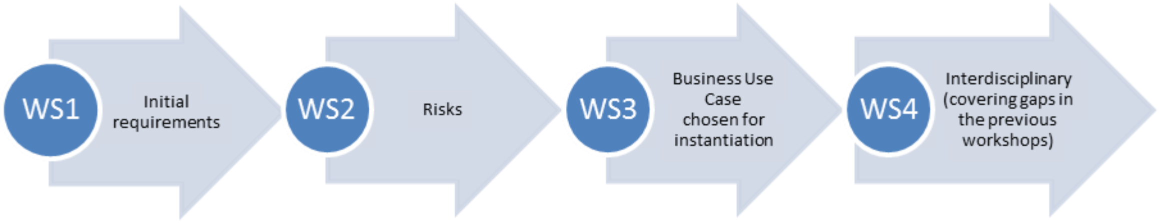

WS1
Initial requirements
WS2
Risks
WS3
Business Use Case chosen for instantiation
WS4
Interdisciplinary (covering gaps in the previous workshops)

**Figure 2: The four stakeholder elicitation workshops and their principal focus.**

The main goal of the first workshop (WS1) was to elicit initial accountability requirements from key stakeholders and to get a reality-check on the three business use cases defined by WP:B-3. In the second workshop (WS2) the main aim was to gather stakeholder views and best practices about the notion of risk and trust in the context of assessment of different types of cloud services.  The third workshop (WS3) was centred on accountability mechanisms, in particular, some of the software tools developed by A4Cloud. WS3 was completed as a set of five sub-workshops held by different project partners, which focused on different aspects of the tools that were reviewed. Finally, the fourth workshop (WS4) exposed the stakeholders to metrics for accountability and incident response management in a cloud computing setting. Furthermore, a small number of external legal experts provided input on high-level descriptions of the tools developed in the project, and gave feedback on how they expected such tools to be received by cloud customers and providers. These four workshops will be further described in Section 2 of this deliverable. In addition, WP 22 has organised a number of additional activities in order to refine and validate the requirements elicited in the four stakeholder elicitation workshops. These activities will also be described in more detail in Section 2.

## 1.3 Deliverable Organisation

The remainder of this report is organised as follows. In Section 2 we describe the elicitation process in detail and provide more information on the various workshops. This section also describes the structure and use of the A4Cloud requirement repository. In Section 3 we present a set of general requirements for cloud providers that we call "the guiding lights requirements". In Section 4 we present an overview over all the requirements currently in the repository as well as an analysis of the requirements. Section **Error! Reference source not found.** discusses our main findings and outlines the further use of the elicited requirements. Section **Error! Reference source not found.** states the main conclusions from the WP 22 Elicitation work package. Appendix A contains a glossary and in Appendix B we describe in detail the results from the last workshop run in the context of the WP 22 Elicitation work package (WS4). Appendix C provides more information on the numbering scheme of the requirement repository. Appendix D lists all the functional accountability requirements currently in the repository, Appendix E lists the requirements elicited specifically for accountability mechanisms and Appendix F lists the requirements in the repository that deal with policy languages for accountability. Finally, Appendix G documents the flow of requirements within the project, illustrating where requirements are created and where they are consumed.

# 2 Requirements Elicitation

This section summarises the elicitation-related activities that have been organised by WP 22. These activities have either generated new requirements (in the four elicitation workshops WS1-WS4) or served to validate and reinforce requirements elicited in earlier stages of the project.

## 2.1 Event Organisation

Figure 3 shows a timeline of the main events that were organised by the WP 22 Elicitation workpackage. As can be seen from the figure, there is a higher frequency of events towards the end of the workpackage span; this is natural since more results became available for presentation to stakeholders as the project progressed.

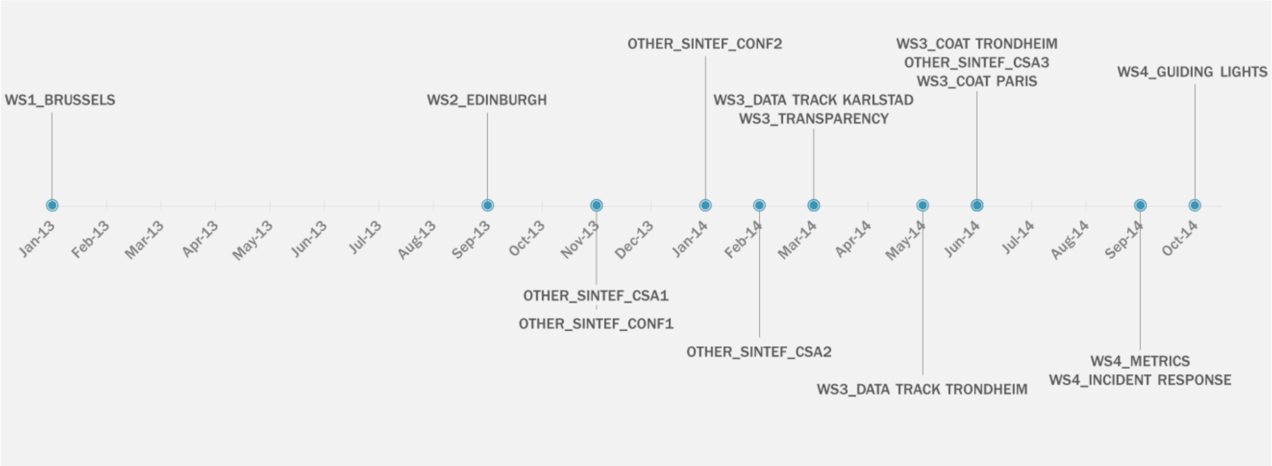


**Figure 3: A timeline of the main events in WP 22 Elicitation.**

The different activities in Figure 3 are listed with a short explanation in Table 1; more details on the elicitation workshops and other activities are given in Section 2.2 and Section 2.3, respectively.

**Table 1: List of WP 22 activities - explanations to Figure 3**

| DATE | ACTIVITY ID | DESCRIPTION |
|---|---|---|
| Jan-13 | WS1_Brussels | WS1 Brussels: initial requirements (7 participants) |
| Sep-13 | WS2_Edinburgh | WS2 A4Cloud Risk Workshop (20 participants) |
| Nov-13 | Other_SINTEF_CSA1 | CSA Norway/Dataforeningen member meeting (19 participants) |
| Nov-13 | Other_SINTEF_Conf1 | How can accountability mechanisms alleviate security and privacy concerns in Cloud Computing? - Trans-Atlantic Science Week (~30 participants) |
| Jan-14 | Other_SINTEF_Conf2 | Security, privacy and accountability in cloud-based medical sensor networks Safecomp2014 (~30 participants) |
| Feb-14 | Other_SINTEF_CSA2 | Health data in the cloud - a healthy idea, or simply sickening? CSA Norway - (~50 participants) |
| Mar-14 | WS3_Transparency | Transparency Interviews (8 participants) |
| Mar-14 | WS3_Data Track Karlstad | Data Track - KAU (20 participants) |
| May-14 | WS3_Data Track Trondheim | Data Track - SINTEF (18 participants) |
| Jun-14 | WS3_COAT Trondheim | COAT - SINTEF (11 participants) |
| Jun-14 | WS3_COAT Paris | COAT - HP (50 participants) |
| Jun-14 | Other_SINTEF_CSA3 | Tools for accountability in the cloud - CSA Norway (50 participants) |
| Sep-14 | WS4_Metrics | Metrics for Accountability - Malaga (20 participants) |
| Sep-14 | WS4_Incident Response | Incident Response in the Cloud - Trondheim (16 participants) |
| Oct-14 | WS4_Guiding Lights | Survey based on Guiding lights QMUL |

## 2.2 The Elicitation Workshops

The main goal of the first workshop (WS1, reported in D:B-2.1 [3]) was to elicit initial accountability requirements from key stakeholders. In addition, the first workshop aimed to get a reality-check on the three business use cases that were planned to demonstrate how the A4Cloud accountability approach can prevent breaches in trustworthiness, detect policy violations, and correct violations that may occur. To elicit requirements we relied on the workshop techniques Open Space Technology [7] and World Cafe[8], because these techniques handle complex situations involving diverse participants and the need for a quick decision-making and make use of face-to-face communication and interaction through active stakeholder participation. Through a workshop based on open processes, led by the stakeholders themselves, 57 initial requirements in the form of accountability relationships were identified. The identified relationships cover the accountability elements assurance, liability, observability, remediation, responsibility, sanctions, transparency and verifiability.

The second workshop (WS2, reported in D:B-2.2 [4]) was concerned with the (perceived) risks associated with cloud services. The main aim of the workshop was to provide a venue where technical experts from the project and stakeholders from the field could exchange their views and best practices about the notion of risk and trust assessment of cloud services, future Internet services and dynamic combinations of such services (mashups). WS2 combined the discussion of relevant information, such as threats to cloud computing, with on-going project work that concerned accountability, risk and trust. In order to engage stakeholders in technical discussions related to the on-going research activities within the project, we organised the elicitation discussions in terms of focus groups. The workshop consisted of four different sessions on accountability, risk and trust (and related topics). Each session exposed the stakeholders to different discussion topics summarised by key questions. These questions guided the discussions of the focus groups, entailing an open form discussion. Based on the discussions at the workshop, 15 requirements related to risk and accountability were identified.

In the third workshop (WS3, reported in D:B-2.3 [5]), we presented the stakeholders with accountability mechanisms (in particular, some of the software tools developed by A4Cloud) in order to gather their operational experiences and expectations about accountability in the cloud. Originally, this workshop was to be organised in the context of the business use case chosen for instantiation, however, due to the project decision to implement a simplified use case specifically defined to showcase all the tools developed in the project, rather than instantiating one of the original three business use cases, WS3 focused on A4Cloud tools rather than on a specific business use case domain. In order to support focused discussions, we organised a set of sub-workshops (rather than a single one) for specific cloud actors: Cloud subjects, Cloud customers and Cloud providers. These groups of cloud actor roles are aligned with the emerging cloud reference architecture (in terms of cloud roles) adopted and extended by the A4Cloud project [15]. Each stakeholder workshop presented and used an accountability mechanism (in some specific cases, a software tool) as a means for stimulating discussions. We demonstrated software tools as a means for gathering feedback, giving stakeholders the opportunity to comment and express their accountability expectations in practice, that is, what they would like to experience (operationally) in the cloud. In all the sub-workshops in WS3 we also exposed the stakeholders to the requirements that we had already elicited in the project, in order to refine them.

The fourth workshop (WS4, reported in Appendix B of this deliverable) was comprised of two main events. The goal of the first event (a workshop on metrics for accountability, which was organised in Malaga, Spain) was to gather feedback from the stakeholders on the main objectives and challenges of the A4Cloud project and the importance of having specific metrics for the A4Cloud attributes and how such metrics can influence accountability. The goals of the second event (a workshop on incident management, which was organised in Trondheim, Norway) was to present the challenges related to incident response that organisations may face when migrating to the cloud, to collect the participants' perceptions on some of the requirements that have already been elicited by CSA [12] and by Brogauer and Schreck [13], and to refine these requirements.

## 2.3 Other Activities

In addition to the conventional elicitation workshops, we have exposed stakeholders to A4Cloud tools and results in a number of more dissemination-oriented events. Although no new requirements per se have been derived from these events, the discussion has served to confirm many of our previously elicited requirements.

In November 2013, we organised a meeting where we presented the core principles of the A4Cloud project in the light of challenges in the cloud ecosystem, and initiated a broader discussion of privacy and confidentiality in the cloud after the NSA PRISM revelations. The 19 participants of this meeting were from CSA Norway[1]/Dataforeningen[2].

In November 2013, the presentation "How can accountability mechanisms alleviate security and privacy concerns in Cloud Computing?" was given at Trans-Atlantic Science Week, Washington DC, to about 30 participants comprising policy makers, technical experts, and industry representatives. This presentation was similar to the one mentioned directly above, and exposed stakeholders to the core principles of the A4Cloud project.

In January 2014 the "health care services in the cloud" business use case was presented at the International workshop on safety & security of (wireless) medical sensor networks. The workshop was organised by TU Delft, the Netherlands. The business use case was presented to an audience consisting of approximately 35 stakeholders from the European public and private health care sector and served as input to a discussion session where safety and security requirements for wireless medical sensor networks were discussed. The insights from the discussion session lead to an improved description of the A4Cloud health care use case.

In February 2014, we ran a workshop with 50 participants from the local IT community in Trondheim, where we focused on personal data protection issues, and we paid particular attention to the obstacles perceived by patients, hospitals, regulators and service providers with respect to outsourcing the processing of healthcare data to public cloud service providers. The workshop consisted of three introductory presentations, which were then followed by a number of focus group sessions that involved a number of stakeholders from the healthcare sector. We have written a paper [14] based on this workshop where we outline a number of obstacles to adoption of public cloud services in the healthcare domain identified by the workshop participants. The paper also discussed our results in light of the previous studies and outlined how current research on cloud accountability may help to solve the identified obstacles. The paper was presented at the ARES Conference 2014.

In June 2014, a snapshot of the most mature A4Cloud tools was presented to a gathering of about 50 technical experts and industry representatives at the CSA Norway summer conference in Oslo, Norway. The presentation inspired discussion both during the event and afterwards.

## 2.4 Internal Dissemination Activities

Apart from eliciting requirements, an important part of WP 22 has been to disseminate the requirements process and the results within the A4Cloud project itself. This was of course done during plenary project meetings, but we also performed more targeted actions. In order to hit the ground running, the first workshop (WS1) was organised already in January 2013 (i.e. three months after the project had started), which proved to be quite challenging not only in terms of recruiting stakeholders (as will be discussed in Section 6), but also in terms of reaching a consensus among the project partners who had not at that time yet had the opportunity to work together. A workshop preparatory meeting was therefore held in Trondheim, Norway, in December 2012 to discuss strategy and agree the techniques and the agenda of WS1.

Since the requirements ultimately are intended for the tool development efforts in stream D, important findings have been regularly disseminated to WP leads by emails; this included our flow of requirements as illustrated in Appendix G and our mapping of requirements from the first two workshops (WS1 and WS2) to the individual work packages.

## 2.5 Requirements Repository

The stakeholder elicitation workshops that were organised by WP 22 resulted in a large number of requirements. In order to categorise them, to classify them with respect to what actor(s) they apply to, to preserve consistency, to simplify future management and to make all the requirements accessible to all the project partners, we created a requirements repository. This will ensure that requirements are effectively communicated to work packages that need them, particularly when these requirements are updated or changed during the course of the project. Furthermore, the repository also serves as the collection point for requirements created by other workpackages in the project.

[1] http://cloudsecurityalliance.no

[2] http://www.dataforeningen.no/in-english.128921.no.html

The requirement repository created for the project has three main objectives:

- Collecting all requirements from all workpackages in a single location;
- Describing all requirements in a uniform manner;
- Providing a global reference for each requirement for tracking purposes.

To meet these objectives we utilised the software versioning and revision control system (SVN) that all project partners have access to, created an Excel spreadsheet template for requirements, and specified a requirement numbering scheme. In Appendix C we describe the requirements template and numbering scheme in detail, as well as the methodology for adding new requirements and updating the existing ones in the SVN.

It is important to note here that the requirements in each elicitation activity must be internally consistent, but no attempt has been made to enforce coherence between requirements in *different* activities; this is a consequence of how the requirements have been gathered and analysed. The Excel sheets do not contain raw text, but the result of extracting individual requirements from (e.g.) workshop minutes. However, the versioning scheme explained in Appendix C caters for an evolution of requirements as they are refined by validation activities in the development work packages.

# 3 Guiding Light Requirements

The following section aims to supplement the requirements elicitation process described in the DoW by providing a set of high-level "guiding light" requirements, formulated as requirements an accountable organisation must meet. Tools to be developed within the project must support organisations in meeting these top level requirements. The guiding light requirements must be read in conjunction with the project scope, objectives, and conceptual model because these jointly define the A4Cloud concept of accountability. These requirements seek to answer the question "What does it take to be an accountable cloud provider?" , and are thus oriented more toward an "organisational" reader than a technical one.

In previous work leading up to the specification of the A4Cloud project, and as part of the conceptual work performed within the project, there are many more or less implicit requirements for accountability that are drawn from the literature and/or the partners' experience. Until the creation of the Guiding lights, there was no formalised process for documenting these requirements, other than hinting that the stakeholder elicitation activities should strive to relate their work to the conceptual framework that is being developed by WP 32 [15].

## 3.1 Rationale

The guiding light requirements were developed by a multidisciplinary group of A4Cloud researchers[3] involved in the various conceptual tasks within the project, taking into account the various documents produced in the project so far as well as relevant external documents (such as the ‘Galway’[16] and ‘Paris’[17] deliverables produced in the CIPL Accountability project).

The starting point is that an accountable organisation must commit to responsible stewardship of other people’s (personal and/or confidential) data. More specifically, the organisation should follow the accountability practices outlined in the A4Cloud conceptual model [15], which in brief entail that the organisation:

- **defines** what it does,
- **monitors** how it acts,
- **remedies** any discrepancies between the definition of what should occur and what is actually occurring
- **explains** and justifies any action.

Basically the first three bullets describe the standard cybernetic loop (define, monitor, correct) as well as the preventive, detective and corrective mechanisms described in the project objectives (see D:C-2.1 [15]).

## 3.2 Guiding Light Requirements

These elements can be elaborated as follows.

1. *Accountable organisations must demonstrate willingness and capacity to be responsible and answerable for their data practices*
   *Data practices* are a shorthand for the processing of data that falls within the scope of the A4Cloud project. This primarily concerns personal data as defined in the Data Protection Directive [18], but may extend to types of confidential information that do not involve personal data.

2. *Accountable organisations must define policies regarding their data practices*
   *Policy* is a shorthand for the wide variety of things that need to be defined by an accountable organisation. Policies may take the form of written text (such as privacy statements or manuals), machine readable policies in a formal language or any form that conveys information about the way the organisation deals with the sensitive/confidential information within scope.
   Aspects of the data practices that need to be defined (may) include:
   - the entities involved in the processing of data and their responsibilities
   - the scope and context of processing data
   - the purposes and means of processing
   - data handling and data access policies

[3] Nick Wainwright (HP), Siani Pearson (HP), Massimo Felici (HP), Martin Gilje Jaatun (SINTEF), Ronald Leenes (Tilburg), Eleni Kosta (Tilburg), Bushra Hasnain (QMUL), Alain Pannetrat (CSA).

- risk monitoring and risk mitigation
- relevant external legal obligations (such as what legal obligations the organisation has in disclosing data to third parties (e.g., in the context of law enforcement)

These items include information obligations as defined in the data protection legal framework, but extend those to include all elements that are relevant for customers to make informed choices about the organisation's offering and that allow checking compliance later on (in the monitoring stage) and will also be based on business considerations related to the service provider's services. Policies hence have external (e.g., the law, social norms) and internal (business objectives) sources that are the relevant ones for the given context.

3. *Accountable organisations must monitor their data practices*
   Accountable organisations outline how they process data and have to be able to prove that they acted according to their policies and hence have to monitor the actual data practices and keep records of the monitoring and its results (i.e. a running account).

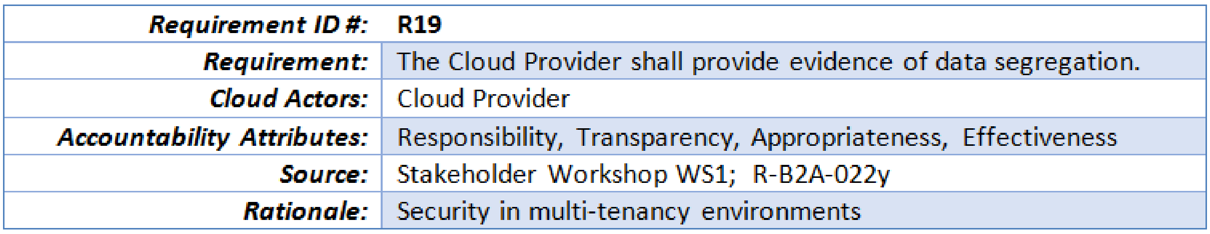
4. *Accountable organisations must correct policy violations*
   If discrepancies between the stated policies and actual (system) behaviour are detected, several things need to be done about it. First of all the *effects* of the violation need to be addressed. Errors need to be corrected and damages need to be compensated (financially or otherwise). Second, the *causes* of the violation need to be addressed. If the violation is the result of a faulty process, the process needs to be repaired, or improved. If the violation results from a data breach or (other) cybercrime, the security needs to be improved, etc. Third, the appropriate stakeholders need to be *informed*. In some cases the authorities (such as the Data Protection Authorities) need to be informed; in other cases the customer or affected data subjects may need to be informed (depending on, for instance, the policies as defined by the organisation).

5. *Accountable organisations must demonstrate policy compliance*
   The final element of the accountability loop is demonstration of compliance with the adopted policies. Not only policy violations need to be reported, an accountable organisation should be willing and able to demonstrate compliance with their policies in a timely fashion "reactively" and where possible "proactively". Furthermore, it should be able to demonstrate that the controls that are selected and used within the service provision chain are appropriate for the context and provide evidence that the operational environment is satisfying the policies (cf. point 3. above).

In addition to the above, there is a need for accountability requirements across the cloud service provision and governance chains and not just in isolation for organisational cloud consumers or cloud service providers, who are the focus of the project scope, described above. Hence there is a need for provision of evidence of satisfaction of obligations right along the service provision chain as well as aspects such as checking that partners are accountable too and that there has been proper allocation of responsibilities along the service provision chain [9]. These requirements need to be reflected within the processes for organisations described above, but in addition there are implications in terms of the way that the accountability governance chains will operate, the scope of risk assessment and the ways in which other stakeholders are able to hold this organisation to account. In complex, dynamic or global situations there needs to be a practical solution for data subjects to obtain both requisite information about the service provision and remediation.

# 4 Accountability Requirements

In this section we summarise all the requirements that have been elicited from the different activities performed by WP 22. Since the requirements repository is currently being used within the project, it is important to note that this overview represents a snapshot of the repository at the time of writing. The repository consists of the consolidated accountability requirements gathered by the different elicitation activities. These include all the requirements that were gathered in the stakeholders elicitation activities performed by WP 22 as well as requirements that other work packages in the project have provided. This section provides a brief summary of these requirements. Appendices D, E and F list the requirements in a tabular format (that is, a simple requirement template tailored to capture relevant information such as the most closely related accountability attributes and cloud actors – corresponding to the definitions given within WP 32 – alongside the requirement description and rationale). This allows grouping and analysing requirements by accountability attributes and cloud actors (who are concerned with the specific requirement). Figure 4 shows an example of a functional requirement (from Appendix D) described using the requirement template tailored to accountability.



| | |
|---|---|
| ***Requirement ID #:*** | **R19** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of data segregation. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-022y |
| ***Rationale:*** | Security in multi-tenancy environments |

**Figure 4: An example of a functional requirement in the repository.**

Most of the requirements that we have identified are related to the actors involved in the cloud service delivery chain. We call these requirements "functional requirements". These will be described in Section 5.1. In addition, the repository contains 15 requirements that are related to the accountability policy language, 22 requirements that are related to the Data Track tool and 11 requirements that are related to the COAT tool. We call these "requirements for accountability mechanisms" since they directly target the technologies and tools that are being developed in the A4Cloud project. These will be described in Section 5.2.

We have adopted the semantics of RFC 2119 [10] for the requirements text, where e.g. SHALL means "that the definition is an absolute requirement of the specification". SHOULD, on the other hand, implies a recommendation "that there may exist valid reasons in particular circumstances to ignore", and is usually preferably avoided in requirements texts.

The remainder of this chapter summarises all the requirements in the repository. Note that we only describe the requirements at a high level in this chapter; a table including a detailed snapshot of all the requirements in the repository (at the time of writing) is included in the appendices, specifically within Appendix D to Appendix F.

## 4.1 Functional Requirements

Functional requirements are requirements that are directly related to the actors involved in the cloud service delivery chain. They are defined as "The [actor] shall..." where [actor] can be any entity involved in a cloud ecosystem, such as a cloud provider or a cloud customer. As will be seen, most of the requirements in the repository apply to cloud providers; however there also exist requirements that are applicable to cloud customers, cloud users, cloud auditors and other relevant parties, such as standardization bodies. Here we present an overview over the functional requirements in the repository, structured in terms of whether they relate to transparency, incident management, security mechanisms, data governance, data protection legislation, policies or audits.

**Transparency.** Most of the functional requirements that we have defined are related to transparency. These requirements state that cloud providers shall be open and informative about the services that they provide. More specifically, they should be transparent about their data processing practices (for example what data they collect, how they process it, where they store it, how long they store it and with whom they may share it), how their customers' data are separated from other customer data, what service providers that are involved in the service delivery chain and how they conform to existing data agreements. Other requirements related to transparency are information about what security mechanisms that they apply, issues related to the ownership of the data and information about how data breaches will be handled.

The transparency requirements are mostly targeting cloud providers; however, there are also some requirements towards the cloud customers. For example, one of the requirements states that the cloud customer shall perform risk assessment when selecting a cloud service provider. The importance of cloud customers being proactive, making sure that all the documentation is in place was also emphasised by the stakeholders.

In relation to transparency, there is also a strong focus on evidence; the requirements state that cloud providers must be able to provide evidence of the provided service levels and data governance practices and that data policies have been applied satisfactorily.

**Incident management.** The repository also contains many requirements related to incident management, i.e. the processes and procedures that define what should happen in case of a (security) incident at the provider's premises that influence the confidentiality, availability or integrity of their customers' data. There are also a number of requirements on evidence related to incident management, for example that the provider shall be able to deliver evidence of successful recovery from a security breach.

Most of the incident requirements are targeting cloud providers; however, there are also a number of requirements on the cloud users. More specifically, for example, the customer needs to identify and evaluate possible approaches to detect and analyse security incidents making sure that they have access to the data sources and information that are relevant for incident detection/analysis.

**Security mechanisms.** Some requirements are related to what security mechanisms that cloud providers should apply. More specifically, the requirements state that cloud providers should safeguard the integrity, confidentiality, availability and traceability of their customers' data and they should have mechanisms in place that ensure data rights management. Data encryption is also explicitly formulated as a requirement.

**Data governance**. The ability to classify customer data, to segregate different customers' data, to specify where customer data is located and the possibility to opt out from data migration has also been explicitly formulated in terms of requirements that apply to the cloud provider. Related to this, there are also a number of requirements that explicitly state that the cloud provider shall provide evidence of their data governance practices.

**Data protection legislation**. There are also a number of requirements related to compliance with data protection legislation and the ability to provide evidence that compliance requirements are being met. Most on these requirements are on the cloud provider with the exception of one requirement that specifically states that cloud auditors, regulators and DPAs shall clarify compliance with extra-territorial legislative regimes.

**Policies**. Related to data processing policies (e.g., privacy policies), the repository also contains requirements that specifically state that the cloud provider shall implement different policies that are tailored to different types of data, legislation and the needs of the customers, and that they shall provide evidence of policy compliance and notifications in case of possible policy violations.

**Audits**. Finally there are a number of requirements related to audits. These are related to how audits shall be performed; who will be responsible for the audit and what certifications are relevant. These requirements are related to cloud providers, customers and standardization bodies.

## 4.2 Requirements for Accountability Mechanisms

Requirements for accountability mechanisms that are currently stored in the repository are requirements that are related to the COAT and Data Track tools and to the accountability policy language that is being developed in the project. Similarly to the functional requirements, these are defined in terms of "The [mechanism] shall..." where [mechanism] is COAT, the Data Track or the policy language.

**Cloud Offerings Advisory Tool (COAT)**. The purpose of the COAT tool is to assist potential cloud customers (SME organisations and individuals) in assessing and selecting cloud offerings, with respect to certain security and privacy requirements [20]. There are currently 11 requirements related to the COAT tool in the repository. These comprise the intended users of the tool and their needs, the tool's ability to adapt to changes in the service offers and the criteria for best practices, and its ability to act as an independent advisor for potential cloud customers. There are also a number of requirements related to the core functionality of the tool itself, for example on how the criteria can be selected and how the results are displayed.

**Data Track**. The Data Track tool is intended to be used by data subjects to get a user-friendly visualization of all personal data they have disclosed to cloud service, with the additional capability to rectify data if necessary [20]. There are currently 22 requirements related to Data Track in the repository. There are mostly related to the intended functionality of the tool, as seen from the user's perspective. More specifically the requirements state how the data will be tracked, what kind of warning messages the tool will display and how deletion of data should be performed. In addition there are also a few requirements on how the tool should secure the personal data that is has access to (the data must be encrypted), the usability of the tool (it should be usable to a diverse set of users), the applicability of the tools in different domains (health data, financial data, personal data) and how the tool will be deployed (locally installed).

**The accountability policy language**. Finally the repository contains requirements on the A4cloud policy language that is being developed. There are currently 15 such requirements, which comprises its ability to support user preferences, rules about data location, access and usage control, delegation capabilities and rules about data retention. There is also a requirement on attaching policies to data (i.e. "sticky policies").

## 4.3 Analysing the Requirements

As has been explained, the requirements in Appendix D, E and F have been categorised as either "functional requirements" or "requirements for accountability mechanisms", where the first category refers to requirements that are directly related to the actors involved in the cloud service delivery chain and the second category refers to requirements that are related to the COAT and Data Track tools and to the accountability policy language that is being developed in the project. Since the different categories of requirements have different targets they will also most likely be useful in different contexts and to different target audiences. We expect that the requirements for accountability mechanisms will be useful for the researchers in the A4Cloud project as well as researchers outside the project who are working on concepts and tools for cloud security, privacy and/or accountability. These requirements may also be useful to the software industry that is developing similar technologies. On the other hand, since the functional requirements are targeting the actors in cloud ecosystems, these requirements have a wider scope; targeting a wide range of aspects (technical, organisational and societal), which are necessary in order to build an accountable cloud ecosystem.

The starting point of the A4Cloud project is that cloud and IT service providers should act as responsible stewards for the data of their customers and users. Most of the functional requirements that are outlined in Appendix D therefore target cloud providers. However, accountability is a wider concept that also includes the organisations that consume cloud services, the end-users of the services, the data subjects whose data is being processed by the services, as well as the organisations that audit, certify and regulate the services. Some of the requirements therefore target other actors in the cloud ecosystem as well.

Most of the requirements in the repository have been specified at a high level. The main reason is that the requirements should be applicable to a broad spectrum of cloud services models that involve the processing of personal and/or business confidential data. By avoiding specifying detailed requirements on how, for example, the different SaaS, PaaS and IaaS services are implemented and operated we can make sure that sure that the requirements cover also other types of service models that may appear. This is in line with the scope of the A4Cloud project, whose focus is not only on today's cloud services but also future IT services. The exception is the requirements for accountability mechanisms, which are detailed enough to be (more or less) directly applied to the technologies and tools that the project is developing. In fact, some of these requirements have already been implemented in the project tools.

Most of the requirements in the repository originate from perceived challenges that the stakeholders associate with existing cloud services, and thus represent features that stakeholders would like to see in a future accountable cloud ecosystem. However, there are exceptions, for example, "*R211 - The Cloud Subject (Cloud Customer) shall be made aware of the data processing and sharing practices of the Cloud Provider*" is something that almost all providers already do (as they provide privacy policies that specify this).

Accountability requirements can also be derived from the current and future data protection legislation. Many of the requirements in the repository are indeed compliant with the existing Data Protection Directive [18], which specifies a number of rules on the processing of personal data in Europe. Even though the Data Protection Directive has not been used as input to the elicitation of the requirements in our repository, it is clear that the stakeholders that were engaged in the elicitation activities are aware of both the rules in the Directive and the context in which it applies. Similarly, some of the requirements that were elicited form the stakeholders include rules that will appear in the proposed new European Union Data Protection Regulation [19].

# 5 Requirements Insights

The elicitation effort of the A4Cloud project has involved more than 300 stakeholders, resulting in 155 stakeholder requirements. Furthermore, WP 22 has spread knowledge to A4Cloud participants about requirements, highlighting that also things they take for granted as common knowledge can indeed be called requirements. Although the main focus for WP 22 has been stakeholder-driven requirements, we have also devised a central requirement repository for collecting requirements from all work packages, ensuring full traceability for future use. We have also initiated an initial analysis and refinement of the stakeholder requirements; but as will be explained below, the ultimate requirements validation can only be performed by the development of activities that will actually *use* the requirements.

WP 22 has as tangible results produced four reports (WS1 [3], WS2 [4], WS3 [5] and this deliverable) and the requirements in the repository. On a wider scale, WP 22 has contributed to project dissemination through participation in workshops, presentation events and social media channels, and has also provided a venue for exposing stakeholders to early results from the project, collecting feedback enabling necessary course adjustments in the research process. For some tools, this feedback was especially helpful to the tool owners to externalise the requirements for the tools, since such requirements were initially not available anywhere, except as tacit knowledge of the tool owners.

The approach to uptake of requirements in the project has differed from WP to WP. The most direct example is WP 36 Risk and Trust Modelling, which was actively waiting for the results from the first workshop (WS1), and that proactively integrated the preliminary stakeholder requirements in their own work. Other WPs have worked more in parallel with the elicitation work in this WP; these WPs have thus provided complementary input to the tool WPs. Even though only half of the WPs in stream B (WP 22 and WP 24) actively created requirements in the repository, the other WPs created other artefacts useful for the tools (the business use cases in WP 23) and provided legal guidance on other results (WP 25). Almost all work packages in the conceptual stream have contributed requirements to the repository, and the one that did not (WP 35) has instead contributed directly to the elicitation work in WP 22 (see requirements activity R-B2E). At the time of writing, there are nearly 300 distinct requirements in the repository.

## 5.1 Coverage of the Goals for this Work Package

The results of WP 22 are in conformance with the goals for the work package. Looking back at Section 1, most task elements have been satisfactorily competed, even though a few proved to be more challenging than foreseen. In the work done in WP 22, we have been able to establish and maintain contact with stakeholders in a frequent manner; through the workshops we have identified and engaged with a number of relevant stakeholder groups, such as data protection commissioners, auditors, consumer groups, trade bodies and SME organisations, including providers in the cloud ecosystem as well as service users. More than 300 stakeholders were exposed to the concepts of the project and the vision of the A4Cloud project. In addition to the direct inputs to the A4Cloud project that were generated, our events have served to strengthen interaction between customers and providers of cloud services, opening up new opportunities for collaboration.

As shown in this deliverable, the workshops were clearly described and organised in such a way that the participants were recruited to contribute actively to the elicitation process of A4Cloud. Participation was very good from the stakeholders who committed to be part of the events. All workshops proved to be fruitful with respect to generating further insights for the tools, accountability practices (or expectations), and for the project in general. Our stakeholder selection and invitation process was suitable for the A4Cloud project, although recruiting stakeholders to non-local events proved more difficult than firs envisaged. When reflecting on the method for generating discussions which led to stakeholder feedback, the methods used through all workshops showed to be effective, and they can favourably be reproduced in other workpackages for further eliciting, evaluating and refining the requirements of the tools to be developed in the project. Such re-use by other workpackages has been facilitated by the very detailed description of the design, running and analysis of the elicitation activities provided in the deliverables [3].

The analysis of the requirements documented in this report expand on the insights generated by the workshops in terms of identifying the participants' perceptions and attitudes towards accountability, and illustrate their expectations in regard to the project.

## 5.2 Moving Forward

The most concrete legacy that WP 22 hands off to the rest of the project is the requirements repository with its associated requirements. The requirements repository is designed with requirements evolution in mind. It is envisioned that some requirements of a general nature may be modified by a tool owner for clarification based on experiences in the development process. Other requirements may be split in two or more, with the resulting requirements being further specialised to fit specific tools. Some requirements may even be deemed out of scope for the tools developed in the project, and left for further work. In general, the tool-producing WPs need to take ownership of the requirements, and will be responsible for any update and maintenance. Although the elicitation WP concludes with this report, further dissemination and demonstration activities both within and outside the project will provide opportunities to expose the tools to internal and external stakeholders, providing both corrective input to the requirements and the tools themselves.

The development WPs will thus implement specific requirements (a subset of the ones identified), and quite likely discover new ones (due to the implementation experiences of integrating all pieces together), and at the same time validate the requirements themselves, in accordance with the traditional software engineering V-model (where the second part of the V focuses on implementation, testing and validation).

Through application in the tool development process we expect that the requirements in the repository will be further improved, and it is therefore important that the development work packages take the time to refine and update the requirements that apply to them. At the end of this process, we expect to be left with a (possibly smaller) set of validated requirements which may subsequently be released to the general community and other accountability-related development efforts.

## 5.3 Concluding Remarks

This deliverable marks the end of the requirements gathering phase in the A4Cloud project. It presents all the requirements that were gathered under the umbrella of WP 22, an analysis of the content of them and explains the methodologies that have been used to elicit them. The main objective of WP 22 has been to ensure that the project activities reflect the needs of the stakeholder groups. The requirements represent this link between stakeholder needs and project activities. The elicitation activities have included a large number of external stakeholders who have been given the opportunity to express their opinions on and experiences with security, privacy, risk and trust issues of public cloud services. In addition, a number of researchers from the A4Cloud project have contributed with additional requirements for the technologies and tools that they are working on. While we overall are happy with the number of stakeholders that have attended the elicitation activities (in particular the WS2 [4] and WS3 [5] events attracted a large number of stakeholders) and the number of requirements that were generated from these events, we can conclude that not all of the identified stakeholders groups have been well represented. We have had a good representation of cloud customers, cloud providers and cloud users in our workshops, focus groups and interviews, but cloud auditors and consumer groups have not been equally well represented.

The requirements repository contains a broad spectrum of requirements that covers a diverse range of technical, organisational and legal constraints. In all nearly 300 requirements have been gathered and analysed. These requirements currently serve as input to the development of the A4Cloud toolset and to the demonstrator that will be used to disseminate the project results. In addition we foresee the requirements to be useful for both other cloud, security and privacy research communities as well as for the software industry that are delivering software and services to be deployed in public and private cloud ecosystems.

The requirements in the repository indicate that transparency is seen as an important attribute of an accountable cloud ecosystem. This is reflected in the large number of requirements that state that cloud providers shall be open and informative about the services that they provide. Incident management is also considered highly important for accountability. The ability to manage security and privacy incidents in a timely manner, and to be open and honest towards the customers and users whose data have been affected by the incidents, is seen as highly important. It is, however, interesting to note that there are also a number of transparency and incident management requirements that target the cloud customers. Accountability is clearly not a one-way concept; all actors in the cloud ecosystem have to cooperate to make it work.

WP 22 has completed its task of eliciting stakeholder requirements related to accountability; it is now up to the development work packages to make the best use of this effort to ensure that the A4Cloud tools reach their highest potential.

## References

[1] Ellen Gottesdiener, Requirements by Collaboration: Workshops for Defining Needs, Addison Wesley, 2002.

[2] A4CLOUD, Accountability For Cloud and Future Internet Services, Annex I, Description of Work, Grant agreement 317550, Version date 2012-09-13.

[3] Nils Brede Moe (Ed.), Stakeholder Workshop 1 Results (Initial Requirements), A4Cloud Project Deliverable D:B-2.1, Version 1.0, March 2013.

[4] Erdal Cayirci (Ed.), Risk Modelling for Cloud Services Workshop Results, A4Cloud Project Deliverable D:B-2.2, Version 1.0, November 2013.

[5] Daniela Soares Cruzes and Massimo Felici (Eds.), Workshop 3 results (Use case domain) - Refining requirements through tools, A4Cloud Project Deliverable D:B-2.3, Version 1.0, July 2014.

[6] Bashar Nuseibeh, Steve Easterbrook, Requirements Engineering: A Roadmap, ICSE '00 Proceedings of the Conference on The Future of Software Engineering, pages 35-46 http://dl.acm.org/citation.cfm?id=336523

[7] Owen, Harrison (2008). Open Space Technology: A User's Guide (3rd ed.). Berrett-Koehler. ISBN 978-1-57675-476-4. (see also http://www-new1.heacademy.ac.uk/assets/documents/heinfe/Open-Space-Technology--UsersGuide.pdf)

[8] World Café Method, http://www.theworldcafe.com/method.html

[9] Martin Gilje Jaatun et al. "Towards Strong Accountability for Cloud Service Providers", Enterprise Security WS, in Proceedings of CloudCom 2014, Singapore

[10] Scott Bradner "Key words for use in RFCs to Indicate Requirement Levels", IETF Network Working Group Request for Comments 2119, March 1997 https://www.ietf.org/rfc/rfc2119.txt

[11] Maartje Niezen (Ed.) "Final report on socio-economic context", A4Cloud Project Deliverable D:B-4.2, September 2014

[12] CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

[13] Bernd Brogauer and Thomas Schreck, Towards Incident handling in the Cloud: Challenges and Approaches, CCSW '10 Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pages 77-86 http://dl.acm.org/citation.cfm?id=1866850

[14] Karin Bernsmed et al., Healthcare Services in the Cloud - Obstacles to Adoption, and a Way Forward. ARES 2014

[15] Massimo Felici and Siani Pearson (Eds.) “Conceptual framework,” A4Cloud Project Deliverable D:C-2.1, September 2014.

[16] Galway Project, “Data protection accountability: The essential elements a document for discussion,” Centre for Information Policy Leadership, October 2009, http://www.huntonfiles.com/files/webupload/CIPL Galway Accountability Paper.pdf.

[17] Paris Project, “Demonstrating and Measuring Accountability - A Discussion Document - Accountability Phase II,” Centre for Information Policy Leadership, October 2010.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:281:TOC

[19] 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 (25 January 2012).

[20] Frederic Gittler and Theo Koulouris (Eds.): "High-level architecture", A4Cloud Project Deliverable D:D-2.2, October 2014

[21] David Nuñez and Carmen Fernandez-Gago (Eds.) "Validation of the Accountability Metrics", A4Cloud Project Deliverable D:C-5.2, October 2014

## Appendix A. Glossary

A complete glossary for the project can be found in **WP:C-2 (Glossary).** This section briefly describes the concepts and terms that are relevant to DB2-1.Some of these are also unique to this deliverable and are not described in the project glossary.

| Term | Definition |
|---|---|
| Accountability | There are many definitions in the main glossary, the short one is “Responsibility of an entity for its actions and decisions.” The working definition of accountability in A4Cloud is based on the Elements of Accountability defined below. |
| Accountability Elements | See Elements of Accountability |
| Accountability relationships | Initial high-level requirements based on stakeholder statements from the workshop. Will later be refined to generate more detailed accountability requirements. |
| Assurance | Assurance is the provision of ex ante evidence for compliance to governing rules |
| Cloud Auditor | A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation |
| Cloud Broker | An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. |
| Cloud Consumer | A person or organisation that maintains a business relationship with, and uses service from, Cloud Providers. |
| Cloud Infrastructure Provider | The provider of the collection of hardware and software that enables cloud computing. |
| Cloud Service Provider | An organisation that provides and maintains delivered cloud services. |
| Cloud Provider | A person, organisation, or entity responsible for making a service available to interested parties |
| Elements of Accountability | A set of concepts that collectively define our notion of accountability. A4Cloud has identified the following elements of accountability: Responsibility, Liability, Transparency, Assurance, Sanctions/Holding to account, Observability, Verification/Validation, and Remediation |
| Liability | Liability can be explained as an obligation (either financially or other penalty) in connection with failure to apply governing rules and/or honoring commitments; liability is an element of almost every definition of accountability |
| Observability | Observability means that the parties can see what is happening; this is closely related to transparency, and to holding to account |
| Open Space Technology (OST) | A workshop technique recommended for complex situations involving a diverse participants and the need for a quick decision making |
| Remediation | Corrective action taken by the accountable organisation in case of failure to apply governing rules and honor commitments |

| Term | Definition |
|---|---|
| Responsibility | Attribution of responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to center on accountability as the quality or state of being held to account for one's actions and an obligation or willingness to accept responsibility for one's actions |
| Retrospective | In software development, a retrospective means a meeting that is held at the end of a project (or completed part of an ongoing process) in order to discuss the successful parts of this effort, and the parts that need improvement. |
| Sanctions/Holding to account | This relates to the presence of sanctions in the case of failure to apply governing rules and honor commitments |
| Stakeholder | In A4Cloud, a stakeholder means a person, group or organisation that affects or can be affected by the A4Cloud project results. |
| Transparency | Describes the property of an accountable system that it is capable of "giving account" of, or providing visibility of how it conforms to its governing rules and commitments |
| Verification/Validation | This is the provision of ex post evidence for compliance to governing rules |
| World Café | Drawing on seven integrated design principles, the World Café methodology is a simple, effective, and flexible format for hosting a large group dialogue. See http://www.theworldcafe.com/method.html |

# Appendix B. Workshop 4

As described in the DoW, WS4 was led by UMA, with participation from SINTEF, HP, QMUL and TiU. Due to difficulties in recruiting a sufficient number of stakeholders to a centralised workshop, it was decided to again organise this elicitation effort as several local events. WS4 workshops, was planned to be an interdisciplinary workshop intended to cover any gaps not resolved by the preceding workshops. There are many gaps that potentially could have been addressed here, but for practical reasons it was decided to focus on accountability metrics, an additional A4Cloud tool (Incident Response), and additional legal input, The goal of the Malaga Workshop on Metrics for Accountability was to expose stakeholders to the main objectives and challenges of the A4Cloud project and the importance of having specific metrics for the A4Cloud attributes and how they influence on accountability. The goal of the Incident Management Workshop was to present the challenges related to incident response that organisations may face when going to the cloud, collect the participants' perceptions on some requirements already elicited by CSA [12] and by Brogauer and Schreck [13], and refine these requirements. The workshops were supplemented by an email consultation survey from QMUL, attempting to gauge how legal experts would react to the Guiding Light requirements; this last activity did not result in new requirements, but provided useful input for the ongoing work in the project.

## B.1 Malaga Workshop on Metrics for Accountability

The goal of this workshop was to present stakeholders the main objectives and challenges of the A4Cloud project and the importance of having specific metrics for the A4Cloud attributes and how they influence on accountability.

Thus, the workshop consisted of two parts. During the first part we gave the audience an overview of A4Cloud and prompted them with several questions for discussion. During the second part we explained to the audience the need for measuring accountability and outlined how this can be done. We then distributed a questionnaire for them to answer. The workshop took place on the 3rd of September 2014 in Malaga.

The invitation was sent to the members of the research community in Computer Science at UMA as well as members of clerical and technical staff. We also invited SMEs working on the area of cloud computing. There were around 30 representatives of each of the sectors that we invited in the workshop.

### B.1.1 Data Collection and Analysis

The data collection for the first part of the workshop comprised three questions that were launched to the audience to generate discussion. The discussions were transcribed by three members of the team at UMA.

The questions that we launched were the following:

- What are your main concerns when using the cloud?
- How important for you is the transparency of cloud provider on the treatment of your data?
- Do you think we are missing any dimension of accountability?

The answers to these questions cannot be interpreted in a quantitative way. We analysed the data from the transcription of the discussions and show them in the next section.

Fort the second part of the workshop the attendees replied to a questionnaire about metrics either online or by filling in a printed version that we distributed to them at the beginning of the session.

### B.1.2 Results

Here we describe the answers to the above questions by the attendees of the workshop. The questions we launched were a way to motivate the audience to start the discussion. The results we obtained are not listed below as answers to any specific questions but as general answers that were provoked by the three questions that we launched.

- The main concerns of the users about moving their data to the cloud is the loss of control over it. Are the data really deleted by the provider when the user does so?
- The issue that most of the large cloud providers are set in the US it is seen by the users as threat to the protection of their data as the providers are not tied to the European regulations on data protection. The main problem is therefore the compliance with legal aspects.
- There is the need to promote the creation of European cloud providers such as the cases of Google or Amazon in the US. There exist cloud providers in Europe but they still act locally in their own areas or countries such as the case of Telefonica in Spain. However, a unique cloud provider market for Europe will be desirable.
- The users should have more control in the cloud. For instance, by giving them the possibility to manage their own security measures. This means the user should have a bigger control on the cloud infrastructure. It is necessary to distinguish between security at the service level from security at the platform level.
- Need for automated audits, more traceability and isolation.
- Another big problem identified by the users is the interoperability of the infrastructures and platforms in the cloud.
- The advantage of using the cloud could be that we could trust that cloud providers have all the mechanisms in place such as trained staff, audits, certifications or specific equipment.
- It is then of paramount importance for the users that the cloud providers guarantee them that they perform audits in a periodic way and obtain appropriate certifications. This will increase the trust in the cloud for potential users.
- A guarantee of the protection of the users' data could be for example to encrypt the data. In this case, the main issues are responsibility and liability. Who is liable for the data, the cloud provider or the user? Could the cloud provider look into the data and check the contents?

### B.1.3 Validation of Accountability Metrics

As mentioned before, one of the parts of the workshop was regarding metrics for accountability, and in particular, about its validation. The catalogue of metrics was presented and feedback from the participants was required. We consider this part of the workshop as the beginning of the process of metrics validation [21].

This process used the Delphi methodology for organizing the collection of feedback from the participants. The Delphi methodology is a structured procedure based on surveys of expert opinions, which is usually used in forecasting and decision-making processes. It requires the participation of a moderator (or a group of moderators), who prepares questionnaires and reviews the responses, and a group of experts, which responds anonymously to the questionnaires. The procedure in the Delphi methodology is iterative; in each round, expert opinion about a certain subject is surveyed by means of the questionnaires. At the end of the round, the moderator reviews the responses, and refines the questions based on the identified consensus and disagreement. The process is repeated several times, until a reasonable consensus is reached, or the moderator believes it is enough.

The validation session that took place in this workshop was intended as a starting point of the validation process, and its output was refined in further rounds of validation. We refer to this session as the “Round 1” of our application of the Delphi methodology. Individual follow-ups for most of the participants (specifically, 14 of the original 18) from the first round, constituted a second round of validation. We refer to this session as “Round 2”.

With regards to the content of the validation session, we prepared a set of questions regarding the accountability metrics catalogue. Given the size of the catalogue, of approximately 40 metrics, we strived to keep the questions short. In our approach, the experts evaluate the metrics catalogue through some general questions, but at the same time are given the liberty of asking or discussing about any particular metric. This way, the size of the questionnaire is kept short, but there is room for discussing specific aspects if needed.

The questionnaire contained three questions in the form of statements about the respondents’ opinions with a five-point scale: strongly disagree (1), disagree (2), neither agree nor disagree (3), agree (4), strongly agree (5). These questions were:

- Q1: "*This set of metrics contains meaningful and relevant measures for Accountability in the Cloud*". With this question, we wanted to analyse the level of appropriateness of the catalogue for measuring the concept of Accountability in the Cloud.
- Q2: "*The use and application of this set of metrics would be easy, in general*". The goal of this question is to assess the perceived degree of feasibility of the metrics proposed.
- Q3: "*This set of metrics can be easily understood by a professional audience*". The goal of this question is to evaluate the degree of usability of the catalogue with respect to the facility of being understood by professionals. We focused on professionals since this part of the stakeholders are the ones that most likely will apply and benefit from the metrics for accountability, due the specialization of some of the metrics. The general public (i.e., cloud end-users) needs much more simplified and aggregated information, so we did not considerate for this question.

The motivation behind the election of these questions was twofold. Firstly, past experience has shown that it is difficult to gather responses to surveys if there are too many questions. Thus, questions should be concise and kept to the minimum. Secondly, we wanted to evaluate the metrics with respect to the most relevant quality criteria for validating the metrics, which in our case are appropriateness, feasibility and usability.

In the original Delphi methodology, the participants are involved through several rounds; however, given the difficulty of engaging a moderately big group of participants during the whole process, we adapted the methodology so the subsequent round after the in-person session was performed individually, in an ad hoc manner. The results of each round were analysed and changes on the catalogue of metrics were made in order to refine the input for the next round.

The validation process took place in two rounds, as prescribed by the Delphi methodology. Response to the questionnaire was, in general, very satisfactory, as shown in Figure A1: question Q1 had a good rating (3.89), much like question Q3 (4.28); the average rating for question Q2 (3.44), although good, was also closer to the neutral value. These results seem to indicate that the presented catalogue is in general well received, but there is a concern with the perceived difficulty of the respondents with respect to the feasibility of applying catalogue. After analysing the free-text comments, this scepticism was due to the feeling that it would be difficult to encourage providers to adopt it. This is discussed further above. In order to obtain a more detailed insight, Figure A2 shows the distribution of responses per option. This distribution is very similar to the result of the online survey, although slightly more diverse.

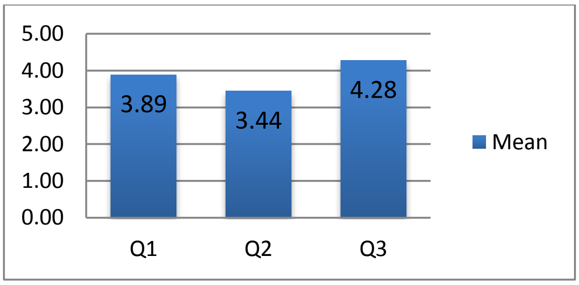


**Figure 5: Average rating of responses (Round 1)**

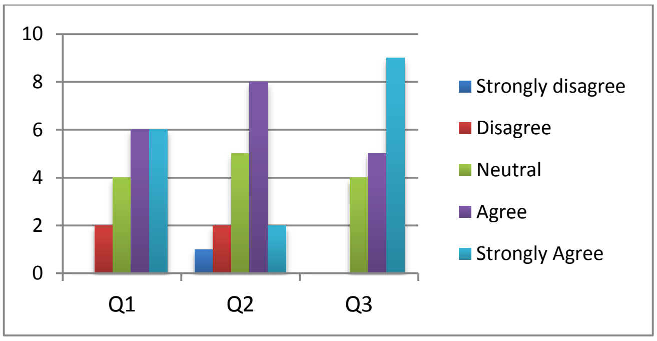


**Figure 6: Distribution of responses per option (Round 1)**

Some of the most remarkable comments received during this session were:

- "*The catalogue is very complete and reflects appropriately several facets of Accountability, however, the difficult part is to engage cloud service providers for utilizing these metrics. I wonder how are you going to tackle this*". Although this comment is not strictly directed to the catalogue itself, we believe is highly relevant for the success of the work package itself.
- *"Several metrics seem to be based on information coming from self assessments, which is not very useful*". Indeed, there are several metrics that are based on evidence that is usually self-assessed. To this end, the confidence on the metrics, as described in D:C-5.2, tries to tackle this issue by expressing the level of independency in the "source of assessment" factor.

Most of the participants of the first round of validation were willing to take part in a second round of validation. Since this round did not imply a huge variation of the catalogue with respect to the previous round, there was no need for repeating an in-person meeting with all the participants. Instead, a refined version of the catalogue, together with better explanation of its objectives and motivation, was distributed individually, and responses were gathered one at a time, as well.

As shown in Figure A3, and with more detail in Figure A4, results were very similar to the previous round, although slightly higher ratings were obtained. This time, question Q1 was rated higher (4.07) than the "Agree" level, which corresponds to a rating of 4. Question Q2 also increased, although it did not surpass the agree level. Rating of question Q3 remained practically the same.

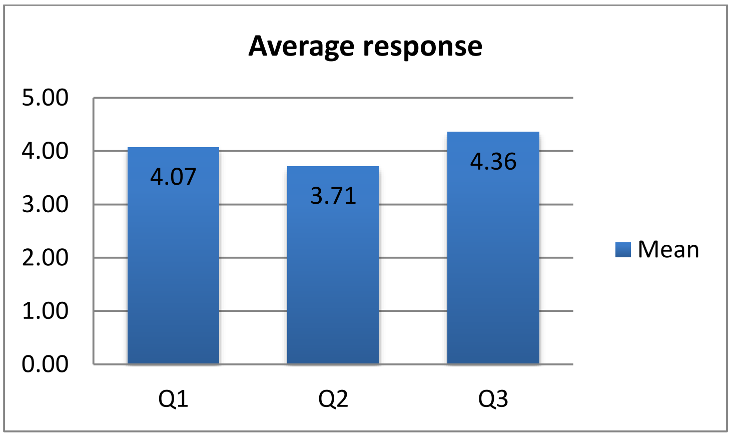


**Figure 7: Average rating of responses (Round 2)**

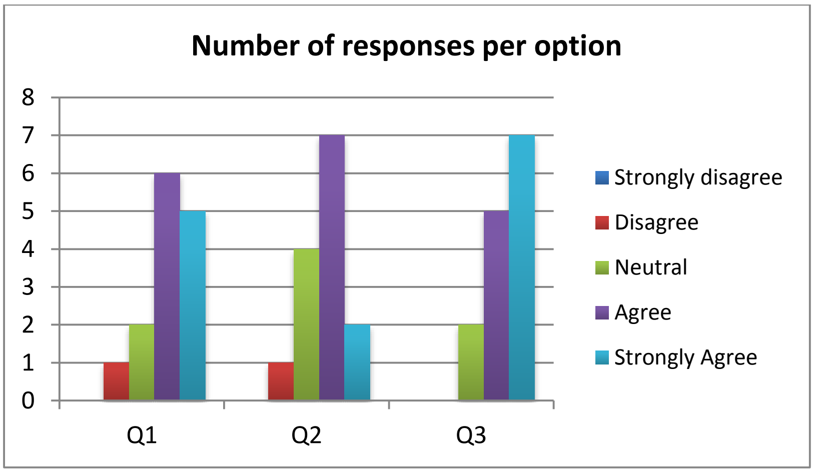


**Figure 8: Distribution of responses (Round 2)**

### B.1.4 Questionnaire

1. Describe your level of agreement or disagreement regarding the following statements about the metrics you reviewed. If you have comments regarding specific metrics, you can use the textbox in the next question, indicating the identifier of the concerned metrics. (Available options: Strongly disagree / Disagree / Neither agree nor disagree / Agree / Strongly agree)
    - Q1: This set of metrics contains meaningful and relevant measures for Accountability in the Cloud
    - Q2: The use and application of this set of metrics would be easy, in general
    - Q3: This set of metrics can be easily understood by a professional audience

2. Additional comments. If you have comments regarding specific metrics, you can write them here indicating the identifier of the concerned metrics. Finally, please let us know if you miss any relevant metric.
3. The next questions are purely optional, but your responses would be very helpful for us.
    - What is the title that best describes your job?
    - In your work, you are best described as a: Cloud customer / Cloud provider / Other (please specify)
    - Would you be interested in a follow up inquiry? If so, please provide your email address.

## B.2 QMUL Questionnaire

Obtaining reactions to A4Cloud’s tool suite from lawyers with experience in the cloud field has proved difficult. A formal survey conducted at the end of September 2007 did not achieve sufficient responses to be useful statistically, and there is little appetite among the legal profession for attending workshops.

In QMUL’s opinion the reasons for this are entirely understandable:

- The work of lawyers is largely reactive to the demands of their clients. If the clients are not seeking advice on accountability, lawyers are not interested in it professionally
- Lawyers are, however, keen to be ready to meet client demands. Informal discussion of accountability generates interest from legal practitioners, but that interest is about tools which already exist and whose uses and implications can be analysed. The work of A4Cloud on its tool suite is still at too early a stage to generate interest from the profession.

This document summarises the views of lawyers practising in the cloud field, as conveyed to QMUL researches in informal and unstructured discussions (eg at conferences) and from the small number of survey responses. Although the information here has not been obtained scientifically, we believe it is accurate so far as it goes and thus likely to be of some use in guiding development of the tool suite. The information is, however, incomplete, and there are certainly matters of concern to practising lawyers which are not reflected here.

### B.2.1 Control and Transparency Tool

In the survey we described this tool as follows:

> This tool would enable a cloud customer to identify how its data (personal data for which it is responsible and confidential information) have been processed in the provider chain, and to exercise some control over that processing.

There was general consensus that cloud customers would welcome such a tool, and that it would assist them in achieving legal and regulatory compliance. However, there was less certainty about the attitude of cloud service providers. Some lawyers thought that providers might be willing to implement the tool in a private cloud, but that in a public cloud scenario there would be less willingness to do so. There was also disagreement how far cloud providers would find the tool helpful in achieving compliance, in part because the degree to which e.g. data protection law applies to public cloud providers is highly uncertain.

One respondent suggested that consumer and SME customers would find the tool of limited use because of their inexperience with both law and technology.

### B.2.2 Choices Tool

> This tool would assist cloud users to make choices between cloud service providers, or between different cloud services, based on the levels of accountability available.

It was generally agreed that customers, at least in the consumer and SME sectors, would be keen to use such a tool. However, there was disagreement about whether it would help those customers to achieve legal and regulatory compliance. Some lawyers think that the differences between national implementations of the law are too complex to be captured in such a tool without making it unworkable (e.g., through asking so many questions at a highly granular a level that it would be usable by the average consumer or SME).

Some lawyers also foresaw both commercial and competition law obstacles. Commercially, much of the information which the choices tool would need from customers is commercially sensitive, so that they might be unwilling to supply it. This could be overcome if there were commercial advantages to doing so, but competition law would require the tool operator to be truly independent of any provider, and thus unable to give that provider commercial advantages.

### B.2.3 Compliance Tool

We described this tool as one which:

> … would generate information about compliance failures in the cloud service chain. The focus would be on (a) the provider’s internal policies, (b) external obligations such as data protection regulation, and (c) external social and ethical norms.

Again, it was thought that customers would welcome such a tool, which would assist them to achieve compliance. There was disagreement whether providers would be willing to adopt the tool – perhaps within a private cloud, but in a public cloud the easy visibility of failures would be a commercial disadvantage as against providers who were not offering the tool. It might also expose providers to regulatory liability by providing evidence of compliance failures.

There was universal agreement that providers would be unwilling to make this information available to other providers, for commercial reasons, and therefore the tool would not be able to work across layering of services.

### B.2.3 Guidelines Tool

> This tool will consistent of integrated technical, legal and organisational guidelines which aim to assist providers and cloud customers in achieving accountability.

Practising lawyers tended to think guidelines would be useful to customers if they could be produced in an accurate and usable form. There was some scepticism about whether that would be possible, but if it were possible then such guidelines would not duplicate existing guidance material, and thus be a real contribution to the achievement of legal and regulatory compliance by customers. It was thought less likely that guidelines would assist providers, because they already take legal advice which addresses their specific compliance issues, and so more general guidelines would not help them.

The most common reaction was that lawyers would want to see the tool in action before passing comment on it. They accepted that guidelines which vastly simplified the technical, legal and organisational issues could still be useful, but this would depend on their content. Guidelines which were sufficiently detailed to capture all elements relevant to legal and regulatory compliance were thought to be unachievable in usable form, and certainly impossible to keep up to date.

### B.2.4 Conclusions

Although the opinion finding described in this section could be considered to be unrepresentative and unscientific, there is an interesting result in its suggestion that the main beneficiaries of the tools are clearly seen to be (a) cloud customers, who furthermore (b) are consumers or SMEs. Little benefit to cloud providers is foreseen.

It is also clear that practising lawyers think that the main obstacles to adoption of the tools will be the potential commercial disadvantages to providers, and the possible increase in their legal risks. It would be worth exploring these issues with providers to identify whether they might be overcome, and if so what safeguards need to be built into the tools.

## B.3 Incident Management Workshop

The goal of this workshop was to present the challenges related to incident response that organisations may face when going to the cloud and to collect the participants' perceptions on some requirements already elicited by CSA [12] and by Brogauer and Schreck [13] and then to refine these requirements. All the material used in the workshop can be found in this appendix.

The invitation was sent to professionals participating in the Norwegian Computer Society (Dataforeningen - DND). This is the largest IT professional association in Norway - an open, independent forum by and for IT-professionals and advanced IT users. DND provides a cohesive environment for practitioners and users of IT subjects. Society's many forums and events will be the preferred forum for strengthening their skills and knowledge transfer and exchange with peers. Participation was voluntary, but returned questionnaires received a movie ticket. The workshop took place on the 16th of September from 17:30 to 20:30 in Trondheim Norway. 16 people attended the workshop, and 14 answered the questionnaire.

### B.3.1 Data Collection and Analysis

As described below, the data collection comprised a questionnaire distributed after the presentation. The questionnaire comprised three main sections. The first two sections asked the participants to assess their agreements with statements on requirements elicited from the CSA Guide [12] and from Brogauer and Schreck [13] respectively. The last section asked the participants to freely write other comments (extra requirements, improvements, suggestions, recommendations, justification of their answers) about the requirements for incident response. All data from the questionnaires were tabulated and analysed quantitatively; all the qualitative data from the session were analysed and also incorporated in the results. All the details of the answers are shown in B.3.3; the main results are shown in the next section.

### B.3.2 Results

As we can see in Table 2 and Table 3, most of the participants agreed or strongly agree with the requirements. Some requirements provoked some neutral answers or a few disagreements, forcing the average to go towards neutral. Therefore we assume these are not as strong requirements as the other ones. The requirements that are strongly recommended are 1, 2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 19, 20 and 21. The ones that seem to need more refinement are: 4, 11, 17, 18 (these are indicated by gray text in the tables); these latter requirements were thus not included in the requirements repository.

Table 2: Agreement on the List of Incident Response Requirements from CSA Guide

| # | Requirement | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|---|
| **1** | Customers should ensure that their cloud service provider has appropriate collection and data separation steps and can provide the requisite incident-handling support | **0** | **1** | **0** | **6** | **8** |
| **2** | Cloud Providers should be aware that they are ensuing legal and regulatory issues related to what must or must not be done during and incident. | **0** | **0** | **0** | **4** | **11** |
| **3** | Customers should ensure that the cloud provider has an up to date Incident Response Plan. | **0** | **2** | **2** | **5** | **6** |
| **4** | Customers should try to integrate as much as possible the providers incident response plan to their own plans. | **0** | **2** | **3** | **8** | **2** |
| **5** | SLAs and contracts should address responsibilities in each phase of IR lifecycle. | **0** | **1** | **1** | **6** | **7** |
| **6** | Customers and providers should consider the means by which sensitive information is transmitted between parties to ensure that data will be securely transmitted. | **0** | **2** | **1** | **1** | **11** |
| **7** | Cloud customers should make sure that they have access to the data sources and information that are relevant for incident detection/analysis. | **0** | **0** | **2** | **8** | **5** |
| **8** | Cloud Customers should make sure that they have access to appropriate forensic support for incident analysis in the cloud environment they are using. | **0** | **1** | **3** | **7** | **4** |
| **9** | The Customers IR team should determine the appropriate logging required to adequately detect anomalous events and identify malicious activity that would affect assets. | **0** | **2** | **1** | **10** | **2** |
| **10** | Cloud customers should conduct an assessment of what logs are available, how they are collected and processed and how and when they may be delivered by the cloud provider. | **0** | **1** | **0** | **13** | **1** |
| **11** | Cloud Customers should understand the forensics requirements for conducting incident analysis, research to what extent the provider meet these requirements. | **0** | **1** | **4** | **8** | **2** |

Table 3: Agreement on the List of Incident Response Requirements from Grobauer and Schreck

| # | Requirement | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|---|
| 12 | Cloud Providers should provide access to controlled event sources and vulnerability information to cloud customers. | 0 | 1 | 1 | 8 | 5 |
| 13 | Especially for PaaS and SaaS, cloud providers should provide access to event data and other information relevant for incident handling via interfaces under the control of the provider. | 0 | 1 | 0 | 8 | 6 |
| 14 | Customers should have a choice to add security-specific event sources required, possibly as service add-on. | 0 | 1 | 1 | 9 | 4 |
| 15 | Incidents that originate with CSP-controlled infrastructure and might have an impact on a customer's resources must be reported to the customer. | 0 | 0 | 3 | 2 | 9 |
| 16 | The SLA must provide a well-defined incident classification scheme and inform about reporting obligations and service levels (what is reported, how fast is reported, etc.) | 0 | 1 | 0 | 8 | 5 |
| 17 | External incident reports that concern or impact a customer must be brought to the attention of the customer with a defined service level. | 0 | 0 | 2 | 9 | 2 |
| 18 | When entering a cloud-sourcing relationship, cloud customers should have at least a basic under- standing of the CSP's infrastructure such that in case of a security incident, information gathering does not "start from zero." The CSP should provide such information to the customer. | 0 | 2 | 2 | 7 | 3 |
| 19 | The customer needs to identify possible approaches to detect and analyse security incidents. | 0 | 0 | 3 | 8 | 4 |
| 20 | The customers should Evaluate CSP's level of support for detection and analysis. | 0 | 0 | 2 | 7 | 5 |
| 21 | The customers and CSPs should establish communication channels and exchange formats of incident information. | 0 | 0 | 2 | 6 | 6 |

### B.3.3 Questionnaire and Answers

## Incident Response in Cloud Computing

**Instructions:** For each of the following statements, mark one box that best describes your opinions on what should be requirements for cloud accountability.

| **Incident Response** | Strongly Disagree | Disagree | Neither | Agree | Strongly Agree | Don’t Know |
|---|---|---|---|---|---|---|
| 1. Customers should ensure that their cloud service provider has appropriate collection and data separation steps and can provide the requisite incident-handling support | □ | □ | □ | □ | □ | □ |
| 2. Cloud Providers should be aware that they are ensuring legal and regulatory issues related to what must or must not be done during and incident. | □ | □ | □ | □ | □ | □ |
| 3. Customers should ensure that the cloud provider has an up-to-date Incident Response Plan. | □ | □ | □ | □ | □ | □ |
| 4. Customers should try to integrate the provider's incident response plan as much as possible into their own plans. | □ | □ | □ | □ | □ | □ |
| 5. SLAs and contracts should address responsibilities in each phase of the Incident Response lifecycle. | □ | □ | □ | □ | □ | □ |
| 6. Customers and providers should ensure that data will be securely transmitted. | □ | □ | □ | □ | □ | □ |
| 7. Cloud customers should make sure that they have access to the data sources and information that are relevant for incident detection/analysis. | □ | □ | □ | □ | □ | □ |
| 8. Cloud Customers should make sure that they have access to appropriate forensic support for incident analysis in the cloud environment they are using. | □ | □ | □ | □ | □ | □ |
| 9. The Customer's IR team should determine the appropriate logging required to adequately detect anomalous events and identify malicious activity that would affect assets. | □ | □ | □ | □ | □ | □ |
| 10. Cloud customers should conduct an assessment of what logs are available, how they are collected and processed and how and when they may be delivered by the cloud provider. | □ | □ | □ | □ | □ | □ |
| 11. Cloud Customers should understand the forensics requirements for conducting incident analysis, research to what extent the provider meets these requirements. | □ | □ | □ | □ | □ | □ |

# Incident Response in Cloud Computing

**Instructions:** For each of the following statements, mark one box that best describes your opinions on what should be requirements for cloud accountability.

| **Incident Response** | Strongly Disagree | Disagree | Neither | Agree | Strongly Agree | Don't Know |
|---|---|---|---|---|---|---|
| 12. Cloud Providers should provide access to controlled event sources and vulnerability information to cloud customers. | □ | □ | □ | □ | □ | □ |
| 13. Especially for PaaS and SaaS, cloud providers should provide  access to event data and other information relevant for incident handling via interfaces under the control of the provider. | □ | □ | □ | □ | □ | □ |
| 14. Customers should have a choice to add security-specific event sources required, possibly as a service add-on. | □ | □ | □ | □ | □ | □ |
| 15. Incidents that originate with CSP-controlled infrastructure and might have an impact on a customer's resources must be reported to the customer. | □ | □ | □ | □ | □ | □ |
| 16. The SLA must provide a well-defined incident classification scheme and inform about reporting obligations and service levels (what is reported, how fast it is reported, etc.) | □ | □ | □ | □ | □ | □ |
| 17. External incident reports that concern or impact a customer must be brought to the attention of the customer with a defined service level. | □ | □ | □ | □ | □ | □ |
| 18. When entering a cloud-sourcing relationship, cloud customers should have at least a basic understanding of the CSP's infrastructure such that in case of a security incident, information gathering does not "start from zero." The CSP should provide such information to the customer. | □ | □ | □ | □ | □ | □ |
| 19. The customer needs to identify possible approaches to detect and analyze security incidents. | □ | □ | □ | □ | □ | □ |
| 20. The customers should Evaluate the CSP's level of support for detection and analysis. | □ | □ | □ | □ | □ | □ |
| 21. The customers and CSPs should establish communication channels and exchange formats of incident information. | □ | □ | □ | □ | □ | □ |

Please provide any comments (extra requirements, improvements, suggestions, recommendations, justification of your answers ) about accountability and incident response.

| Part. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 |
| **2** | 4 | 4 | 3 | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | 4 | 3 | 1 | 4 | 3 | 3 |
| **3** | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 3 | 4 | 4 | 4 |
| **4** | 4 | 4 | 4 | 3 | 4 | 2 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 2 | 3 | 3 | 2 | 4 | 4 | 4 |
| **5** | 3 | 3 | 2 | 3 | 3 | 4 | 3 | 2 | 3 | 3 | 2 | 2 | 4 | 3 |  | 3 |  | 3 | 3 | 2 | 4 |
| **6** | 3 | 4 | 4 | 2 | 2 | 4 | 2 | 3 | 1 | 3 | 3 | 1 | 4 | 1 | 2 | 3 | 2 | 4 | 2 | 3 | 2 |
| **7** | 4 | 4 | 2 | 3 | 3 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 3 | 4 | 3 | 3 | 3 | 3 | 3 | 3 |
| **8** | 3 | 3 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 3 | 4 |
| **9** | 4 | 4 | 4 | 1 | 3 | 4 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 3 | 3 |
| **10** | 4 | 4 | 3 | 3 | 3 | 4 | 3 | 2 | 2 | 3 | 2 | 3 | 3 | 2 | 4 | 3 |  |  | 3 |  |  |
| **11** | 4 | 4 | 4 | 1 | 3 | 3 | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 2 |
| **12** | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |  | 3 | 3 | 2 | 3 | 3 |
| **13** | 3 | 4 | 3 | 2 | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 3 | 4 | 3 |
| **14** | 3 | 4 | 3 | 3 | 4 | 4 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 4 | 4 | 3 | 2 | 3 | 3 | 3 |
| **15** | 1 | 3 | 1 | 2 | 1 | 1 | 3 | 3 | 1 | 1 | 1 | 3 | 1 | 3 | 2 | 1 | 2 | 1 | 2 | 2 | 4 |
| **Average** | **3,73** | **3,82** | **3,36** | **2,73** | **3,36** | **3,73** | **3,36** | **3,18** | **2,91** | **3,09** | **2,82** | **3,09** | **3,45** | **3,00** | **3,18** | **3,27** | **2,55** | **2,64** | **3,27** | **3,00** | **3,00** |

**The tool**

1.Customers should ensure that their cloud service provider has appropriate collection and data separation steps and can provide the requisite incident-handling support
2.Cloud Providers should be aware that they are ensuring legal and regulatory issues related to what must or must not be done during and incident.
3.Customers should ensure that the cloud provider has an up-to-date Incident Response Plan.
4.Customers should try to integrate the provider's incident response plan as much as possible into their own plans.
5.SLAs and contracts should address responsibilities in each phase of the Incident Response lifecycle.
6.Customers and providers should ensure that data will be securely transmitted.
7.Cloud customers should make sure that they have access to the data sources and information that are relevant for incident detection/analysis.
8.Cloud Customers should make sure that they have access to appropriate forensic support for incident analysis in the cloud environment they are using.
9.The Customer's IR team should determine the appropriate logging required to adequately detect anomalous events and identify malicious activity that would affect assets.
10.Cloud customers should conduct an assessment of what logs are available, how they are collected and processed and how and when they may be delivered by the cloud provider.
11.Cloud Customers should understand the forensics requirements for conducting incident analysis, research to what extent the provider meets these requirements.
12.Cloud Providers should provide access to controlled event sources and vulnerability information to cloud customers.
13.Especially for PaaS and SaaS, cloud providers should provide access to event data and other information relevant for incident handling via interfaces under the control of the provider.
14.Customers should have a choice to add security-specific event sources required, possibly as a service add-on.
15.Incidents that originate with CSP-controlled infrastructure and might have an impact on a customers resources must be reported to the customer
16.The SLA must provide a well defined incident classification scheme and inform about reporting obligations and service levels
17.External incident reports that concern or impact a customer must be brought to the attention of the customer with a defined service level.
18.When entering a cloud-sourcing relationship, cloud customers should have at least a basic understanding of the CSP's infrastructure
19.The customer needs to identify possible approaches to detect and analyze security incidents.
20.The customers should Evaluate the CSPs level of support for detection and analysis.
21.The customers and CSPs should establish communication channels and exchange formats of incident information.

## Appendix C. Describing All Requirements in a Uniform Manner

All requirements are placed in a single directory placed in a folder at the top level of the project SVN, where a single Excel spreadsheet is created for each requirement gathering activity. To be specific, a single file should be created for each unique [workpackage,activity] pair. Note that no version is required since all requirements are stored in a single file, including deprecated or obsolete versions. It is the responsibility of each work package to maintain the requirements generated within it. The naming convention is:

- Requirements-WPA.xlsx
  with "WP" replaced by the workpackage that elicited the requirement, and "A" replaced by a letter identifying the elicitation activity within that workpackage; e.g., Requirements-B2A.xlsx (the first activity in WP 22) or Requirements-C4B.xlsx (the second activity in WP:C-4).

The project provides a template that must be used to describe requirements, as described in the following. The use of that template is required, and all relevant fields must be filled-in for each requirement.

In order to keep the full history within the file, no entry must ever be erased in the file. For example, if a change is being made in a requirement that would cause a change in the version of the requirement, the line containing the latest version must be duplicated, the revision must be incremented (e.g. from a to b then to c etc…) and the changes must be done on the duplicated line. The state of the requirement in the original line must be marked as “replaced”, and the identifier for the new requirement must be filled-in in the appropriate column.

Each requirement will be associated with a unique identifier, built in the following manner:

R-WPA-NNNv (e.g. R-B2A-014c or R-C4B-020y)

where:

- R- is the letter R (as in Requirement) followed by a dash
- WP is the identifier for the (leading) work package generating the requirement in a letter+number form (e.g. B2, C4,…) without any separator
- A is a letter used to separate generating activities within a single work package (starting with A for the first generation activity)
- - is a dash
- NNN is a 3 digit number used to identify the requirement in the set, allocated sequentially from 001. If required, this can be extended to 4 digits.
- v is a lowercase letter used to identify the version of the requirement. Requirements with provisional status have letters allocated downward from z to m, requirements with confirmed status have letters allocated upward from a through l.

There are a few additional points to consider on the allocation of these identifiers:

- identifiers should NEVER be reused – when a requirements gets deprecated or cancelled, the identifier remains with the deprecated requirement and is not re-cycled to identify another requirement
- numbers do not capture any structure – if, for example, R-B2B-015b gets split in two requirements, R-B2B-015b will be “replaced” by R-B2B-320a and R-B2B-321a (assuming 320 is the first unallocated number at the time the requirement is being split)
- versions are only to identify clarifications in the description of the requirement. If the requirement was previously misinterpreted and referred to in A4Cloud documents, the corrected definition

should be allocated a new reference number. Simple spelling mistakes or trivial grammatical errors can typically be corrected in-place, without a change of version.

- workpackages should only use a new generating activity identifier if there is no intention to keep coherence between the two lists. If, for example, a work package holds a workshop to define a base set of requirements followed by a second workshop to identify additional requirement for that list, the new requirements should be captured in the same list, under the same generating activity identifier. However, if a work package performs a requirement elicitation activity for the benefit of a given ”consumer” work package, followed by an independent elicitation activity for another ”consumer” work package, with no expectation to have an integrated coherent list of requirements across the two activities, each should be allocated a separate activity identifier.
- Requirements generating activities are politely reminded that confirmed requirements within a list MUST be coherent with the Guiding Light requirements and with other requirements on the same list. There is however no requirement for coherence across.

All activities using a requirement as a justification for the decisions taken or the work done, for example in requirements analysis, are required to explicitly mention the identifiers of the requirements referred to. This will allow searching across all project deliverables for the use of requirements in later phases of the project, identifying how the project is responding to the requirements.

The other fields in the requirements template are used as follows:

**Field STATE –** “tentative” (version z through m), “confirmed” (version a through l), “replaced” (the requirement is replaced by one or more other ones, listed in the appropriate box), “removed” (removed with no successor). Note that a requirement change from “tentative” to “confirmed” is a change of version and therefore requires the duplication of the line as explained above.

**Field SUCCESSOR –** list separated with commas of all requirements identifiers which are replacing this one. Used only in the “replaced” state.

**Field PREDECESSOR –** List separated with commas of all requirements identifiers which are being replaced by this one. Can be used in any state.

**Fields for DATES –** Two fields are available: DATE_CREATED and DATE_RETIRED, respectively for the creation in “tentative” or “confirmed” state, and for the retirement as either “replaced” or “removed”. Note that the state changes from “tentative” to “confirmed” and from “replaced” to “removed” are not possible, and that state changes from “removed” to “tentative” or “confirmed” should not happen.

**Field REQUIREMENT TEXT –** The actual requirement text

**Field STAKEHOLDERS –** Which stakeholders are affected by the requirement; select among the specified ones, or fill in free text in the "other" box if you have identified a new stakeholder

**Field RATIONALE –** The background and reason for the requirement

**Field SOURCE (TRACING) –** Where does the requirement come from (stakeholder workshop, regulation, etc.)

**Field ACCOUNTABILITY ATTRIBUTES –** As defined by C2 - select among the specified ones, or fill in free text in the "other" box if you have identified a new accountability attribute

**Field NOTES –** any additional information about the requirement

# Appendix D. Functional Requirements

This section lists the main elicited requirements. The nature of these requirements is such that they are concerned with the functional elements of accountability. However, they have been classified for relevance in terms of Cloud Actors (affected by the specific requirement) and Accountability Attributes (as requirements explicitly or not influence specific accountability attributes). Future project activities will allow us to validate such requirements and to understand analytically subtle contingencies among them (and the relevant aspects of accountability).

| ***Requirement ID #:*** | **R1** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall implement appropriate organisational security measures in order to safeguard data integrity, availability, confidentiality and traceability. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Verifiability, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-058z |
| ***Rationale:*** | Security of data on behalf of cloud subjects and cloud customers |

| ***Requirement ID #:*** | **R2** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall implement appropriate technical security measures in order to safeguard data integrity, availability, confidentiality and traceability. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Verifiability, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-059z |
| ***Rationale:*** | Security of data on behalf of cloud subjects and cloud customers |

| ***Requirement ID #:*** | **R3** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide data segregation in order to safeguard control over data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-003y |
| ***Rationale:*** | Ability to support data segregation in multi-tenancy environments. |

| ***Requirement ID #:*** | **R4** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall comply with data protection laws. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-004y |
| ***Rationale:*** | The Cloud Provider is liable to other cloud actors, e.g. Cloud Customers, Cloud Auditors and Cloud Supervisory Authorities, for compliance with data protection laws. |

| ***Requirement ID #:*** | **R5** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall implement different policies tailored to the nature of data, privacy laws and needs of the Cloud Customer (Cloud Subject). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, verifiability, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-005y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R6** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence that data policies have been applied satisfactorily. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-006y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R7** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide awareness-related mechanisms to Cloud Customers (Cloud Subjects) that access cloud services for personal data, flagging up any policy violation (e.g. non-compliances with policies). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-007y |
| ***Rationale:*** | Being aware of data policy compliance (violation) |

| ***Requirement ID #:*** | **R8** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide the Cloud Customer with suitable audit mechanisms without compromising data security. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-008y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R9** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall conduct risk analysis with the involvement of cloud experts identifying how security threats expose cloud vulnerabilities. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-010y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R10** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide mechanisms for control and management over data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-011y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R11** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall make it possible for the Cloud Customers (Cloud Subjects) to recover from security attacks. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-012y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R12** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide mechanisms needed for the recovery from security attacks. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Responsiveness, Remediability, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-013y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R13** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of the recovery from security attacks. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability, Observability, Attributability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-014y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R14** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of provided service levels and data governance practices. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-016y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R15** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall only use data for the intended purposes. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-018y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R16** |
| ***Requirement:*** | The Cloud Provider shall comply with security mechanisms with respect to legislative regimes. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-019y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R17** |
| ***Requirement:*** | The Cloud Provider shall implement suitable security mechanisms throughout the data management lifecycle. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-020y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R18** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to legislative regimes without exposing security vulnerabilities. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-021y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R19** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of data segregation. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency,  Verifiability, Attributability, Observability, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-022y;  Work Package C8; R-C8A-015y |
| ***Rationale:*** | Security in multi-tenancy environments |

| | |
|---|---|
| ***Requirement ID #:*** | **R20** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance of data segregation with respect to legislative regimes. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Transparency,  Verifiability, Attributability, Observability, Appropriateness, Effectiveness, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-023y;  Work Package C8; R-C8A-014y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R21** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to legislative regimes for specific industry or public sectors. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |

| | |
|---|---|
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness, Liability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-024y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R22** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide maintenance and provision of security mechanisms. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility,  Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-025y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R23** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide rights management on data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility,  Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-026y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R24** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide mechanisms specifying what operations are allowed on data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility,  Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-027y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R25** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide real time information on physical data storage of different types of data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-028y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R26** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide (real time) information on data storage location of different types of data. |
| ***Cloud Actors:*** | Cloud Provider,  Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-029y;  Stakeholder Workshop WS3;  R-B2C-017z; Work Package C8;   R-C8A-011y |
| ***Rationale:*** | Conformance to Data Agreements; The Cloud Provider shall provide geographical information of where data are stored. |

| ***Requirement ID #:*** | **R27** |
|---|---|

| | |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide timely notification and provision of evidence of data breaches. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-030y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R28** |
| ***Requirement:*** | The Cloud Provider shall provide necessary actions to data breach. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-031y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R29** |
| ***Requirement:*** | The Cloud Broker shall provide evidence of service orchestration. |
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-032y;  R-B2A-034y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R30** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of service orchestration. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-033y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R31** |
| ***Requirement:*** | The Cloud Provider shall provide data classification mechanisms supporting different data security levels (e.g. confidential or non-confidential). |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-035y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R32** |
| ***Requirement:*** | The Cloud Provider shall provide custom-made data security levels. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-036y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R33** |
| ***Requirement:*** | The Cloud Broker shall provide evidence of non-data aggregation (or effective data segregation). |
| ***Cloud Actors:*** | Clod Broker |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-037y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R34** |
| ***Requirement:*** | The Cloud Provider shall comply with competition laws (non-cooperation) in the provision of services. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-038y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R35** |
| ***Requirement:*** | The Cloud Provider shall provide evidence compliance with competition laws (non-cooperation) in the provision of services. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-039y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R36** |
| ***Requirement:*** | The Cloud Provider shall provide the highest data security level as default. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-040y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R37** |
| ***Requirement:*** | The Cloud Provider shall comply with local legislations for international data transfers. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-041y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R38** |
| ***Requirement:*** | The Cloud Provider shall provide a data migration opt-out option. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Verifiability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-042y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R39** |

| | |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to extraterritorial legislative regimes. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-043y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R40** |
|---|---|
| ***Requirement:*** | Cloud Auditors and Cloud Supervisory Authorities shall clarify any compliance with respect to extraterritorial legislative regimes. |
| ***Cloud Actors:*** | Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-044y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R41** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of organisational practices and structures. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-045y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R42** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall allow the use of data encryption. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-046y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R43** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide alternative cloud deployments (i.e. private, community, public and hybrid) and custom-made Service Level Agreements (SLAs). |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-047y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R44** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of data collection practices. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-048y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R45** |
|---|---|

| | |
|---|---|
| ***Requirement:*** | The Cloud Provider shall comply with data collection practices with regulatory regimes. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility, Liability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-049y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R46** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall get explicit consent for any operation on data. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-050y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R47** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall get explicit consent every time any operation is performed on data. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-051y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R48** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall revoke data consent if requested. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-052y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R49** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence that revoked consent has been acted on in a reasonable manner. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-053y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R50** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of data collection practices. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transaprency, Verifiability, Attributability, Observability |
| ***Source:*** | Stakeholder Workshop WS1; R-B2A-054y |

| | |
|---|---|
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R51** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of who has the authority to investigate any policy compliance. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-055y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R52** |
| ***Requirement:*** | The Cloud Provider is liable (also in terms of compensation) to the Cloud Customer (Cloud Subject) for data breaches. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Liability, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-056y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R53** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of data gathered, inferred or aggregated. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS1;  R-B2A-057y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R54** |
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) where the data have been moved to in the cloud |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS2;  R-B2B-001z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R55** |
| ***Requirement:*** | The Cloud Provider shall provide information  if and from whom purchases services  to the Cloud Customer |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS2;  R-B2B-002z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R56** |
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) who is responsible for the various aspects of handling owned data |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |

| | |
|---|---|
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-003z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R57** |
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) about any “conflict of interest” towards data from the provider's side |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-004z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R58** |
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) about storage in other countries and compliance issues related to this storage with respect to laws and regulations of both the other country and their own country. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-005z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R59** |
| ***Requirement:*** | Cloud Providers shall provide evidence that they are maintaining the data in the correct way. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-006z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R60** |
| ***Requirement:*** | The cloud provider, when providing evidence, shall be able to offer selective disclosure (e.g. through a trusted third party) to prevent inadvertent disclosure of third-party confidential information. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-007z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R61** |
| ***Requirement:*** | The Cloud Provider shall be explicit about which data have been collected on the Cloud Customer (Cloud Subject). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-008z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R62** |
| ***Requirement:*** | The Cloud Provider shall demonstrate that they have implemented controls to mitigate organised insider attacks. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-009z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R63** |
| ***Requirement:*** | The Cloud Provider shall provide information facilitating risk assessment. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-010z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R64** |
| ***Requirement:*** | The Cloud Provider shall prove they can take care of data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness, Verifiability, Attributability, Observability |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-011z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R65** |
| ***Requirement:*** | The Cloud Provider shall show trust information provided by third parties. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-012z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R66** |
| ***Requirement:*** | one of the requirements states that the cloud customer should perform risk assessment (if necessary, by third party help) when selecting the Cloud Provider. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-013z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R67** |
| ***Requirement:*** | The Cloud Customer shall trust providers based on regular independent audit (e.g. certifications). |
| ***Cloud Actors:*** | Cloud Customer, Cloud Auditor |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-014z |

| | |
|---|---|
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R68** |
| ***Requirement:*** | The Cloud Auditor (Cloud Supervisory Authority) shall provide a list of certifications required to the Cloud Provider. |
| ***Cloud Actors:*** | Cloud Auditor, Cloud Supervisory Authority, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS2; R-B2B-015z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R69** |
| ***Requirement:*** | The Cloud Provider shall show clear statements of what is possible to do with the data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-001z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R70** |
| ***Requirement:*** | The Cloud provider shall allow the Cloud Customer (Cloud Subject) to choose what is possible to do with the data. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-002z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R71** |
| ***Requirement:*** | The Cloud Provider shall inform (have a page that informs) the Cloud Customer about specific security mechanisms (e.g., firewalls, backup, etc.). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-003z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R72** |
| ***Requirement:*** | The Cloud Provider shall have a standardised description (or language) of the security certification level provided in order to facilitate the Cloud Customer evaluating what security level is needed. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-004z |
| ***Rationale:*** | What is possible to do with the data; what is required from us and what is the provider offering. |

| | |
|---|---|
| ***Requirement ID #:*** | **R73** |

| | |
|---|---|
| ***Requirement:*** | The Cloud Provider shall have a document explaining the procedures for leaving the service and taking the data out from the service. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-005z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R74** |
| ***Requirement:*** | The Cloud Provider shall have a document that describes the ownership of the data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-006z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R75** |
| ***Requirement:*** | The Cloud Provider shall have policies written in a language that the Cloud Customer (Cloud Subject) can understand. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-007z |
| ***Rationale:*** | What is possible to do with the data |

| | |
|---|---|
| ***Requirement ID #:*** | **R76** |
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer on how to protect data or how data are protected. This information is expressed in more details for organisational Cloud Customers rather than for individual Cloud Subjects. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-008z |
| ***Rationale:*** | Correction of the Data |

| | |
|---|---|
| ***Requirement ID #:*** | **R77** |
| ***Requirement:*** | The Cloud Provider shall have a document that describes the adopted mechanisms for securing data against data loss as well as data privacy vulnerabilities. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-009z |
| ***Rationale:*** | Correction of the Data |

| | |
|---|---|
| ***Requirement ID #:*** | **R78** |
| ***Requirement:*** | The Cloud Provider shall have a document describing the procedures and mechanisms planned in cases of security breaches on customer's data. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability |

| | |
|---|---|
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-010z |
| ***Rationale:*** | Correction of the Data |

| | |
|---|---|
| ***Requirement ID #:*** | **R79** |
| ***Requirement:*** | The Cloud Provider, in case of security breaches, shall inform the Cloud Customer (Cloud Subject) on what happened, why it happened, what the procedures the cloud provider is taking to correct the problem and when services will be resumed as normal. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-011z |
| ***Rationale:*** | Correction of the Data |

| | |
|---|---|
| ***Requirement ID #:*** | **R80** |
| ***Requirement:*** | The Cloud Provider shall provide functional, technical and security information about how data are handled. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-012z |
| ***Rationale:*** | Data Handling |

| | |
|---|---|
| ***Requirement ID #:*** | **R81** |
| ***Requirement:*** | The Cloud Provider shall provide information of how the data are stored and who has access to them. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-013z |
| ***Rationale:*** | Data Handling |

| | |
|---|---|
| ***Requirement ID #:*** | **R82** |
| ***Requirement:*** | The Cloud Provider shall make available the technical documentation on how data are handled, how they are stored, and what procedures are for accessing them. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-014z |
| ***Rationale:*** | Conformance to Data Agreements; Having this documentation available it helps. |

| | |
|---|---|
| ***Requirement ID #:*** | **R83** |
| ***Requirement:*** | The Cloud Provider shall have documentation of procedures (expressed at different levels of abstraction) for different cloud actors (e.g. technical staff or cloud subjects). |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-015z |
| ***Rationale:*** | Conformance to Data Agreements |

| | |
|---|---|
| ***Requirement ID #:*** | **R84** |

| | |
|---|---|
| ***Requirement:*** | The Cloud Provider shall show that comply with the data handling agreement concerned with the specific type of data in question. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-016z |
| ***Rationale:*** | Conformance to Data Agreements |

| ***Requirement ID #:*** | **R85** |
|---|---|
| ***Requirement:*** | Cloud software and services shall have monitoring mechanisms for showing the status of the data. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-018z |
| ***Rationale:*** | Conformance to Data Agreements |

| ***Requirement ID #:*** | **R86** |
|---|---|
| ***Requirement:*** | The Cloud Provider, in case of using services from third parties, shall inform the Cloud Customer (Cloud Subject) on the responsibilities of the different parties involved in the agreement. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-019z |
| ***Rationale:*** | Value Chain |

| ***Requirement ID #:*** | **R87** |
|---|---|
| ***Requirement:*** | The Cloud Provider, in case of using services from third parties, shall inform the Cloud Customer about the existence of sub-providers, where they are located and whether they comply with the legal requirements of the country of the cloud customer. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Liability |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-020z |
| ***Rationale:*** | Value Chain |

| ***Requirement ID #:*** | **R88** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer in cases of multi-tenant services. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-021z |
| ***Rationale:*** | Multi-Tenancy |

| ***Requirement ID #:*** | **R89** |
|---|---|
| ***Requirement:*** | The Cloud Provider, in cases of multi-tenant services, shall inform the Cloud Customer how separation from other customers is implemented and guaranteed. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-022z |

| | |
|---|---|
| ***Rationale:*** | Multi-Tenancy |

| ***Requirement ID #:*** | **R90** |
|---|---|
| ***Requirement:*** | The Cloud Provider, in case of multi-tenant services, shall inform the Cloud Customer how it assured that data from one customer will not be accessed by another customer. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-023z |
| ***Rationale:*** | Multi-Tenancy |

| ***Requirement ID #:*** | **R91** |
|---|---|
| ***Requirement:*** | The Cloud Providers shall get the consent of the Cloud Customer (Cloud Subject) before moving data to another country, in cases of new parties involved in the value chain and in cases of changes in the initial terms of contract. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-024z |
| ***Rationale:*** | Decisions and Information during Service |

| ***Requirement ID #:*** | **R92** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall give sufficient information to the Cloud Customer (Cloud Subject) about any change (to the service provided) and the impact of such change to the Cloud Customer (Cloud Subject). This information shall make the Cloud Customer (Cloud Subject) aware of the risk implied by the change. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-025z |
| ***Rationale:*** | Decisions and Information during Service |

| ***Requirement ID #:*** | **R93** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall give information about where data are located, if the cloud provider has connections with other companies or operates in other countries. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-026z |
| ***Rationale:*** | Decisions and Information during Service |

| ***Requirement ID #:*** | **R94** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall have detailed information of the data collected about the Cloud Customer (Cloud Subject). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-027z |
| ***Rationale:*** | Decisions and Information during Service |

| | |
|---|---|
| ***Requirement ID #:*** | **R95** |
| ***Requirement:*** | The Cloud Provider shall make available information in websites about the reputation, recommendations and reviews by the Cloud Customer (Cloud Subject). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-028z |
| ***Rationale:*** | Decisions and Information during Service |

| | |
|---|---|
| ***Requirement ID #:*** | **R96** |
| ***Requirement:*** | The Cloud Customer shall ensure that the Cloud Provider has appropriate collection and data separation procedures and can provide incident-handling support. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-001z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R97** |
| ***Requirement:*** | The Cloud Provider shall be aware of the possibility of ensuing legal and regulatory issues related to what must or must not be done during an incident. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Liability, Remediability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-002z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R98** |
| ***Requirement:*** | The Cloud Customer shall ensure that the Cloud Provider has an up to date Incident Response Plan. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-003z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R99** |
| ***Requirement:*** | The Service Level Agreement (SLA) and business contracts shall clarify and be concerned with the responsibilities involved in each phase of an incident response lifecycle. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transaprency, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-004z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R100** |
| ***Requirement:*** | The Cloud Customer and the Cloud Provider shall consider the means by which sensitive information is transmitted between parties to ensure that data will be transmitted securely. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |

| | |
|---|---|
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-005z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R101** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall make sure having access to the evidence and sources that are relevant for incident detection and analysis. |
| ***Cloud Actors:*** | Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-006z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R102** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall make sure having access to appropriate forensic support for incident analysis in the cloud environment used. |
| ***Cloud Actors:*** | Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-007z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R103** |
|---|---|
| ***Requirement:*** | The Cloud Provider's incident response team shall determine the appropriate logging required to adequately detect anomalous events and identify malicious activity that would affect assets. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-008z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R104** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall conduct an assessment of what logs are available, how they are collected and processed and how and when they may be delivered by the Cloud Provider. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-009z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R105** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall allow the Cloud Customer access to controlled event sources and vulnerability information. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-010z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R106** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide access to event data and other information relevant for incident handling via interfaces under the control of the provider. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-011z |
| ***Rationale:*** | Incident Management;  This is relevant especially for PaaS and SaaS. |

| ***Requirement ID #:*** | **R107** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall have a choice to add security-specific event sources required, possibly as service add-on. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-012z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R108** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer about incidents that originate with the CSP-controlled infrastructure and might have an impact on customer's resources. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-013z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R109** |
|---|---|
| ***Requirement:*** | The Service Level Agreement (SLA) shall provide a well-defined incident classification scheme and inform about reporting obligations and service levels (e.g. what is reported, how fast is reported, etc.) |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-014z |
| ***Rationale:*** | Incident Management |

| ***Requirement ID #:*** | **R110** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall identify possible approaches to detect and analyse security incidents. |
| ***Cloud Actors:*** | Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness, Responsiveness, Remediability |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-015z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R111** |
| ***Requirement:*** | The Cloud Customer shall evaluate the Cloud Provider's level of support for detection and analysis. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-016z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R112** |
| ***Requirement:*** | The Cloud Customer and the Cloud Provider shall establish communication channels and exchange formats of incident information. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2D-017z |
| ***Rationale:*** | Incident Management |

| | |
|---|---|
| ***Requirement ID #:*** | **R113** |
| ***Requirement:*** | The cloud provider must ensure that data is actually deleted when the user performs a delete operation |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-001z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R114** |
| ***Requirement:*** | The cloud provider must enable users to manage their own security measures in the cloud |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-002z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R115** |
| ***Requirement:*** | The cloud provider must distinguish security at the service level from security at the platform level |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-003z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R116** |
| ***Requirement:*** | The cloud provider must support automated audits that provide more traceability |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-004z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R117** |
|---|---|
| ***Requirement:*** | The cloud provider must perform periodic audits |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-005z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R118** |
|---|---|
| ***Requirement:*** | The cloud provider must obtain appropriate certifications |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Appropriateness, Effectiveness |
| ***Source:*** | Stakeholder Workshop WS4; R-B2E-006z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R119** |
|---|---|
| ***Requirement:*** | The Cloud Provide shall provide good insight in the way personal data are treated. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-001z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R120** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) when governments (or local authorities) access personal data |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-002z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R121** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall inform the Cloud Customer (Cloud Subject) when the police accesses personal data. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-003z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R122** |
|---|---|
| ***Requirement:*** | The Cloud Customer (Cloud Subject) may be consulted by the Cloud Provider on how the cloud customer (subject) wants the personal data be handled in the cloud. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-004z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R123** |
| ***Requirement:*** | The Cloud Provider shall make the terms of service comprehensible. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-005z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R124** |
| ***Requirement:*** | The Cloud Provider shall make the privacy policies comprehensible. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-006z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R125** |
| ***Requirement:*** | A legal framework shall steer the proper handling of information in the cloud. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Liability, Appropriateness, Effectiveness |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-007z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R126** |
| ***Requirement:*** | The Cloud Customer shall be able to correct, rectify, block or erase any personal data that has been disclosed. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility, Responsiveness, Remediability |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-008z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R127** |
| ***Requirement:*** | The Cloud Provider shall be responsible for the way personal data is handled in the cloud. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Work Package B4; Survey Outcome; R-B4A-009z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R128** |
| ***Requirement:*** | An independent certification agency should steer accountable behaviour of cloud service providers via certification. |
| ***Cloud Actors:*** | Cloud Supervisory Authority, Cloud Provider |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Work Package B4;  Modelling Task ; R-B4A-010z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R129** |

| | |
|---|---|
| ***Requirement:*** | An independent certification agency should monitor the accountability levels of cloud service providers. |
| ***Cloud Actors:*** | Cloud Supervisory Authority, Cloud Auditor |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Work Package B4; Modelling Task; R-B4A-011z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R130** |
| ***Requirement:*** | In a service provision chain it shall be clear who is liable to the cloud customer. |
| ***Cloud Actors:*** | Cloud Customer |
| ***Accountability Attributes:*** | Liability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-001z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R131** |
| ***Requirement:*** | In a service provision chain responsibility shall be clearly allocated to specific cloud actors. |
| ***Cloud Actors:*** | Cloud Customers, Cloud Providers |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-002z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R132** |
| ***Requirement:*** | In a service provision chain it shall be possible for (a combination of) the cloud auditor to have observability over all parts of the service provision chain. |
| ***Cloud Actors:*** | Cloud Auditor, Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Verifiability, Observability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-003z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R133** |
| ***Requirement:*** | In a service provision chain it shall be possible to attribute specific actions or objects to specific cloud actors. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Verifiability, Attributability, Observability, |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-004z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R134** |
| ***Requirement:*** | In a service provision chain remediation for specific failures shall be a clearly defined process that is easy for the Cloud Customer (Cloud Subject) to apply and that can be ensured. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsiveness, Remediability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-005z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R135** |
| ***Requirement:*** | In a service provision chain the information available to the cloud actors involved follows principles of transparency and ease-of-access. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Transparency |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-006z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R136** |
| ***Requirement:*** | In a service provision chain cloud actors shall be able to verify that specific actions have taken place in any part of the chain. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-007z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R137** |
| ***Requirement:*** | In a service provision chain cloud actors shall be able to verify compliance with specific policies. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-008z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R138** |
| ***Requirement:*** | In a service provision chain there shall be binding and enforceable written data governance policies and procedures that reflect applicable laws, regulations and industry standards. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Liability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-009z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R139** |
| ***Requirement:*** | In a service provision chain executive oversight and responsibility for data privacy and protection shall be clearly allocated. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Transaprency |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-010z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R140** |
| ***Requirement:*** | In a service provision chain all parties are involved in ongoing risk assessment and mitigation supporting the implementation of a process to assist cloud actors in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks. |
| ***Cloud Actors:*** | |

| | |
|---|---|
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-011z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R141** |
| ***Requirement:*** | In a service provision chain all parties are involved in a program of risk assessment oversight and validation, involving a periodic review of the maturity of the program to determine whether modification is necessary. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Transparency, Appropriateness, Effectiveness |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-012z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R142** |
| ***Requirement:*** | With respect to a service provision chain there shall be procedures with clear responsibilities allocated for responding to inquiries, complaints and data protection breaches. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-013z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R143** |
| ***Requirement:*** | In a service provision chain remedies are clearly identified for those whose privacy has been put at risk. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability, Appropriateness, Effectiveness |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-014z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R144** |
| ***Requirement:*** | In a service provision chain all parties carry out risk analysis and mitigation based on their understandings of their obligations and responsibilities. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability, Appropriateness, Effectiveness |
| ***Source:*** | Work Package C2 Conceptual Framework; R-C2A-015z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R145** |
| ***Requirement:*** | In a service provision chain all parties provide evidence that specific mitigations have been implemented in order to address emergent risks. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability, Appropriateness, Effectiveness |

| | |
|---|---|
| ***Source:*** | Work Package C2 Conceptual Framework;  R-C2A-016z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| ***Requirement ID #:*** | **R146** |
|---|---|
| ***Requirement:*** | In a service provision chain all parties should provide evidence that privacy and security controls used are appropriate and adequate for the context. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability, Appropriateness, Effectiveness |
| ***Source:*** | Work Package C2 Conceptual Framework;  R-C2A-017z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| ***Requirement ID #:*** | **R147** |
|---|---|
| ***Requirement:*** | The Cloud Auditor and The Cloud Supervisory Authority involved in the policy enforcement chain shall be responsible to societal institutions (e.g. such as regulators). |
| ***Cloud Actors:*** | Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsibility |
| ***Source:*** | Work Package C2 Conceptual Framework;  R-C2A-018z |
| ***Rationale:*** | Accountability across the cloud supply chain |

| ***Requirement ID #:*** | **R148** |
|---|---|
| ***Requirement:*** | The risk analysis should include ethical, privacy, and compliance considerations. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C2 Conceptual Framework;  R-C2A-019z |
| ***Rationale:*** | Scope of the risk analysis |

| ***Requirement ID #:*** | **R149** |
|---|---|
| ***Requirement:*** | There shall be shared and well-defined semantics for security and privacy attributes. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-001z |
| ***Rationale:*** | Interoperability across the cloud supply chain |

| ***Requirement ID #:*** | **R150** |
|---|---|
| ***Requirement:*** | There shall be shared and well-defined metrics for security and privacy attributes. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-002z |
| ***Rationale:*** | Interoperability across the cloud supply chain |

| ***Requirement ID #:*** | **R151** |
|---|---|
| ***Requirement:*** | The shall be a language which is able to express: |

| | |
|---|---|
| | a. Policies describing constraints and rules applicable to security and privacy attributes including where applicable:<br>I. Purpose definition and limitation;<br>II. Security measures (confidentiality, integrity, availability, key management, purpose limitation measures, etc.);<br>III. Retention and deletion quality;<br>IV. Access control to data by privileged and non-privileged staff;<br>V. Mechanisms for the exercise of user rights (information, modification and deletion)<br>VI. The location of data in relation to applicable law;<br>VII. Transfer of data and/or policies to third parties;<br>VIII. Mechanisms for the implementation of consent and withdrawal of consent, where applicable.<br>b. Scope of Responsibility for data handling policy elements, with the identification of the corresponding parties taking responsibilities for data stewardship.<br>c. Scope of Liability.<br>d. Obligations regarding:<br>I. The process of reporting (Observability, Transparency)<br>II. The process of demonstration (Verifiability, Attributability)<br>III. iii. The process of remediation (Remediability). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Liability, Observability, Transaprency, Verifiability, Attributability, Remediability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-003z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R152** |
|---|---|
| ***Requirement:*** | There shall be a protocol between the two parties, formalising the acceptance of the terms potentially after negotiation, thereby establishing responsibility and liability. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsibility, Liability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-004z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R153** |
|---|---|
| ***Requirement:*** | There shall be a protocol to describe the general policy applied by the Cloud Provider to data provided by the Cloud Customer, and/or, where applicable, specifics terms that apply to the Cloud Customer as negotiated. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-005z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R154** |
|---|---|

| | |
|---|---|
| ***Requirement:*** | There shall be a protocol to report performance and compliance indicators relative to the terms of the agreement reached. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-006z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R155** |
| ***Requirement:*** | There shall be a protocol to report data breaches from the Cloud Provider to the Cloud Customer. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsibility, Transparency, Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-007z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R156** |
| ***Requirement:*** | There shall be a language to describe evidence that supports claims related to the terms of the agreement reached, along with a supporting protocol to:<br>I. Query evidence gathered by the Cloud Provider for verification by the Cloud Customer (Attributability, Verifiability).<br>II. Query evidence gathered by a trusted third party (Cloud Auditor), and provided to the Cloud Customer by the Cloud Provider (Attributability, Verifiability) |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-008z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R157** |
| ***Requirement:*** | There shall be a protocol that enables the cloud Customer to directly test claims made by the Cloud Provider (Observability). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-008z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R158** |
| ***Requirement:*** | There shall be a language that describes the certification by a trusted party of claims made, along with a protocol for the Cloud Customer to verify the authenticity of the certificate. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-008z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R159** |

| | |
|---|---|
| ***Requirement:*** | There shall be a protocol to submit requests for remediation and receive information on the outcome of the request. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-009z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R160** |
| ***Requirement:*** | There shall be a language equivalent for the purpose of describing data stewardship practices to the Cloud Supervisory Authority. |
| ***Cloud Actors:*** | Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-010z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R161** |
| ***Requirement:*** | There shall be an acceptance (or rejection) protocol for prior authorization (or consultation respectively) from the Cloud Supervisory Authority. |
| ***Cloud Actors:*** | Cloud Supervisory Authority |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-011z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R162** |
| ***Requirement:*** | There shall be a severity assessment methodology that allows describing policy deviations along with a common set of metrics to evaluate the apparent severity of a breach based on the deviation. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-012z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R163** |
| ***Requirement:*** | There shall be a protocol for the Cloud Customer (Cloud Subject) to submit data breach notifications to the Cloud Supervisory Authority. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-013z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R164** |
| ***Requirement:*** | There shall be a language to describe evidence that supports claims related to the terms of the agreement reached along with a supporting protocol to:<br>I. Query evidence gathered by the Cloud Provider/Customer for verification by the Auditor/Regulator (Attributability, Verifiability). |

| | |
|---|---|
| | II. Query evidence gathered by a trusted third party (another Cloud Auditor), and provided to the Auditor/Regulator by the Cloud Provider/Customer (Attributability, Verifiability). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Transparency, Attrivutability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-014z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R165** |
| ***Requirement:*** | There shall be a protocol that enables the Cloud Auditor/Cloud Supervisory Authority to directly test claims made by the Cloud Provider/Customer (Observability). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Transparency, Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-014z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R166** |
| ***Requirement:*** | There shall be a language that describes the certification by a trusted party of claims made, along with a protocol for the Cloud Auditor/Cloud Supervisory Authority to verify the authenticity of the certificate. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Transparency, Attrivutability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-014z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R167** |
| ***Requirement:*** | There shall be a notification protocol from the Cloud Supervisory Authority to the Cloud Customer/Provider requesting actions to remediate the effect of a compliance failure, describing:<br>a. The compliance failure that was identified.<br>b. The requested corrective actions, including short terms corrections and long term corrections.<br>c. c. Timeframe requirements for the corrections to be implemented. |
| ***Cloud Actors:*** | Cloud Supervisory Authority, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-015z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R168** |
| ***Requirement:*** | The Cloud Broker shall be able to interpret policy requirements, potentially enhancing them based on its own added value. |

| | |
|---|---|
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-016z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R169** |
| ***Requirement:*** | The Cloud Broker shall be able to execute a protocol to negotiate policy requirements, both with the Cloud Provider and the Cloud Customer. |
| ***Cloud Actors:*** | Cloud Broker, Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-017z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R170** |
| ***Requirement:*** | The Cloud Broker shall be able to report a relevant subset of the general or negotiated policy. |
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-018z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R171** |
| ***Requirement:*** | The Cloud Broker shall be able to aggregate, relay and report the compliance and performance indicators. |
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-019z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R172** |
| ***Requirement:*** | The Cloud Broker shall be able to relay data breach notification. |
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-020z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R173** |
| ***Requirement:*** | The Cloud Broker shall be able to aggregate and relay demonstration requests between the Cloud Customer and The Cloud Provider, potentially adding its own demonstrations. |
| ***Cloud Actors:*** | Cloud Broker, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-021z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R174** |

| | |
|---|---|
| ***Requirement:*** | The Cloud Broker shall be able to modify and dispatch remediation requests, while presenting a central remediation request entry point. |
| ***Cloud Actors:*** | Cloud Broker |
| ***Accountability Attributes:*** | Responsibility, Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-022z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R175** |
|---|---|
| ***Requirement:*** | There shall be a language for the purpose of describing data stewardship practices from the point of view of the Cloud Subject. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-023z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R176** |
|---|---|
| ***Requirement:*** | There shall be a protocol to negotiate elements of the policies between the Cloud Provider and the Cloud Customer tailored to the interests and needs of the Cloud Subject. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-024z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R177** |
|---|---|
| ***Requirement:*** | There shall be a Cloud Subject friendly control interface for the policy language. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-025z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R178** |
|---|---|
| ***Requirement:*** | There shall be a protocol to query information in a Cloud Subject friendly format, presenting the general data policy and/or specific terms agreed. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-026z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R179** |
|---|---|
| ***Requirement:*** | There shall be a protocol to present compliance level information in a Cloud Subject friendly format, for the terms agreed. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-027z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R180** |
| ***Requirement:*** | There shall be an alert protocol that allows the Cloud Subject to be informed about a breach should one occur. Such an interface should at least provide information about the nature of the breach and actions that the Cloud Subject can take to mitigate effects of the breach. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability, , R-C3A-028z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R181** |
| ***Requirement:*** | There shall be a language to describe evidence that supports claims related to the terms of the agreement reached, along with a supporting protocol to:<br>I. Query and verify evidence gathered by the Cloud Provider for verification by the Cloud Consumer (Attributability, Verifiability).<br>II. Query and verify evidence gathered by a trusted third party (Cloud Auditor), and provided to the Cloud Customer by the Cloud Provider (Attributability, Verifiability). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-029z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R182** |
| ***Requirement:*** | There shall be a protocol that enables the Cloud Subject to directly test claims made by the Cloud Provider (Observability, Verifiability). |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-029z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R183** |
| ***Requirement:*** | There shall be a language that describes the certification (or trust-mark) by a trusted party of claims made, along with a protocol for the Cloud Subject to verify the authenticity of the certificate. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Attributability, Verifiability, Observability |
| ***Source:*** | Work Package C3 Interoperability, R-C3A-029z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R184** |

| | |
|---|---|
| ***Requirement:*** | There shall be a protocol for the Cloud Subject to submit requests for remediation to the Cloud Provider/Cloud Customer and receive information on the outcome of the request. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-030z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R185** |
| ***Requirement:*** | There shall be an entry point for the Cloud Subject to submit complaints to the Cloud Supervisory Authority about compliance failures of the Cloud Provider/Cloud Customer. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Supervisory Authority, Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Responsiveness, Remediability |
| ***Source:*** | Work Package C3 Interoperability,  R-C3A-031z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R186** |
| ***Requirement:*** | There shall be machine-readable representation of trust and risk models. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling; R-C6A-001y |
| ***Rationale:*** | Associate risk analysis to event monitoring, automate treatment by tools |

| | |
|---|---|
| ***Requirement ID #:*** | **R187** |
| ***Requirement:*** | There shall be a representation of cloud actors' assets. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-002y |
| ***Rationale:*** | It shall be possible capturing each cloud actor's assets, specifically private and other sensitive data. |

| | |
|---|---|
| ***Requirement ID #:*** | **R188** |
| ***Requirement:*** | It shall be possible modelling trust relationships. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-003y |
| ***Rationale:*** | Provide a representation usable for modelling of trust relationships and delegations in the cloud supply chain |

| | |
|---|---|
| ***Requirement ID #:*** | **R189** |
| ***Requirement:*** | There shall be separate risk profiles. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-004y |

| | |
|---|---|
| ***Rationale:*** | Provide separate risk profiles for different stakeholders: cloud consumers, cloud providers, cloud brokers. |

| ***Requirement ID #:*** | **R190** |
|---|---|
| ***Requirement:*** | It shall be possible modelling cloud ecosystems. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-005y |
| ***Rationale:*** | Encapsulate cloud and accountability concepts (main parties, deployments model, service supply chains, security (accountability) controls). |

| ***Requirement ID #:*** | **R191** |
|---|---|
| ***Requirement:*** | It shall be possible dynamic risk monitoring. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-006y |
| ***Rationale:*** | Associate risk analysis with event monitoring in order to determine impact and the risk thresholds in different cloud landscapes. Constantly update the risk and trust model based on the new events |

| ***Requirement ID #:*** | **R192** |
|---|---|
| ***Requirement:*** | It shall be possible modelling risk and trust of different cloud ecosystems. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-007y |
| ***Rationale:*** | the models must support realistic use cases, composed of multiple cloud service providers, as defined in WP:B-3 |

| ***Requirement ID #:*** | **R193** |
|---|---|
| ***Requirement:*** | It shall be possible representing vulnerabilities and threats. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6A-008y |
| ***Rationale:*** | Be able to represent explicitly in the risk and trust models specific vulnerabilities and threats |

| ***Requirement ID #:*** | **R194** |
|---|---|
| ***Requirement:*** | It shall be possible performing impact assessments. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6B-001y |
| ***Rationale:*** | The Data protection impact assessment tool assesses the impact of specific events from cloud environment (using accountability metrics from WP:C-5). |

| ***Requirement ID #:*** | **R195** |
|---|---|

| | |
|---|---|
| ***Requirement:*** | It shall be possible performing risk estimation. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6B-002y |
| ***Rationale:*** | Estimate the risk levels (using accountability metrics from WP:C-5). |

| ***Requirement ID #:*** | **R196** |
|---|---|
| ***Requirement:*** | It shall be facilitated the section of a Cloud Provider. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6B-003y |
| ***Rationale:*** | Facilitate the selection of a Cloud Provider matching customer's business needs and risk profile |

| ***Requirement ID #:*** | **R197** |
|---|---|
| ***Requirement:*** | It shall be possible supporting contractual negotiations. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C6 Risk and Trust Modelling;  R-C6B-004y |
| ***Rationale:*** | Support the negotiations of contract terms and SLAs based on the risk profile. |

| ***Requirement ID #:*** | **R198** |
|---|---|
| ***Requirement:*** | It shall be made explicit data disclosures and implicit data collections transparent. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R199** |
|---|---|
| ***Requirement:*** | It shall be made data sharing and data processing along the cloud chain transparent, and provide the means to verify it. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Verifiability, Observability |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R200** |
|---|---|
| ***Requirement:*** | It shall be provided indicators for the trustworthiness of cloud actors along the service supply chain. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R201** |
|---|---|

| | |
|---|---|
| ***Requirement:*** | Policies need to make the possible consequences of data disclosures in different recurrent situations transparent. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transaprency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R202** |
|---|---|
| ***Requirement:*** | It shall be made explicit that a service is a cloud-based service and what this implies in terms of privacy/security for the intended Cloud Customer/Cloud Subject. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R203** |
|---|---|
| ***Requirement:*** | There shall be provided easily comprehensible policies informing The Cloud Subject at least about the identity of the Cloud Customer/Cloud Provider, other responsible parties, for what purposes the data will be used plus other details needed, so that they can understand the implications. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R204** |
|---|---|
| ***Requirement:*** | It shall be made trust-enhancing indicators intuitive, consistent and believable, as well as be appealing for the appropriate Cloud Customer/Cloud Subject group. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R205** |
|---|---|
| ***Requirement:*** | Cloud Customers shall know the approach and consequences when deciding to end a cloud service. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R206** |
|---|---|
| ***Requirement:*** | The Cloud Customer (Cloud Subject) shall be aware of the extent to which can act under pseudonyms. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |

| | |
|---|---|
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R207** |
|---|---|
| ***Requirement:*** | The Cloud Customer shall be informed about the termination of their contract in a clear and straight-forward manner. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R208** |
|---|---|
| ***Requirement:*** | It shall be possible making reasonable claims about the privacy and security policies and technical capabilities of the specific cloud service (Cloud Provider) to promote trust. |
| ***Cloud Actors:*** | Cloud Provider,  Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R209** |
|---|---|
| ***Requirement:*** | Cloud Subjects (Cloud Customers) shall be aware of their rights, and shall be supported to exercise their rights; in particular, control options shall be made available and relevant in certain situations more obvious at those particular situations. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R210** |
|---|---|
| ***Requirement:*** | Provide clear statements of what rights apply to individual Cloud Subjects (Cloud Customers) considering different factors, such as their culture or location and applicable legal regime. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R211** |
|---|---|
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be made aware of pros and cons of their possible choices in an unbiased manner. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R212** |
|---|---|
| ***Requirement:*** | It shall be obtained Cloud Subjects (Cloud Customers)' informed consent by helping and motivating them to understand policies and service agreements, so that they understand the implications. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R213** |
|---|---|
| ***Requirement:*** | Graphical User Interfaces (GUIs) for preference settings need to make consequences in different recurrent situations and risks and benefits of disclosure transparent. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R214** |
|---|---|
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be made aware of pros and cons of choices in a comprehensible and unbiased manner. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R215** |
|---|---|
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be able to do settings at the moment when it is relevant (on-the-fly management of privacy settings). |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R216** |
|---|---|
| ***Requirement:*** | Consequences shall be explained not in technical terms, but in practical terms ('speak the Cloud Subject/Cloud Customer's language') |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R217** |
|---|---|
| ***Requirement:*** | It shall be possible for organisational Cloud Customers to negotiate what is negotiable, and make negotiation clear and simple. |
| ***Cloud Actors:*** | |

| | |
|---|---|
| ***Accountability Attributes:*** | Cloud Customer, Cloud Provider |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R218** |
| ***Requirement:*** | Opt-in alternatives shall be provided, e.g. in regard to the country/legal regime of the data storage location. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R219** |
| ***Requirement:*** | Cloud Subjects (Cloud Customers) shall be made aware of their ex post transparency rights, so that they understand and can exercise their right of access. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R220** |
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be made aware of what information the Cloud Provider has implicitly derived from disclosed data. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R221** |
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be made aware of the data processing and sharing practices of the Cloud Provider. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R222** |
| ***Requirement:*** | The Cloud Subject (Cloud Customer) shall be helped in making data traces transparent and promoting subjects/customers' legal rights (e.g. by providing graphical interactive visualisations). |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Liability |
| ***Source:*** | Work Package C7;  Deliverable D:C-7.1 |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R223** |

| | |
|---|---|
| ***Requirement:*** | It shall be provided a standard way to perform audits across the chain of services. In particular, audit functions shall be provided that visualise differences of Service Level Agreements (SLAs_ along the cloud supply chain. |
| ***Cloud Actors:*** | Cloud Auditor |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R224** |
|---|---|
| ***Requirement:*** | Audit functions shall be provided that make also implicitly collected data transparent. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R225** |
|---|---|
| ***Requirement:*** | Cloud Subjects (Cloud Customers) shall be allowed classifying their data items and easily provide access control rules for these data. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R226** |
|---|---|
| ***Requirement:*** | Cloud Customers and Cloud Providers (system administrators) shall be allowed verifying the accuracy of access control rules in a straightforward and simple manner. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C7; Deliverable D:C-7.1 |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R227** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence that data policies have been applied satisfactorily. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C8; R-C8A-001y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R228** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of the recovery from security attacks. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Responsiveness, Remediability |

| | |
|---|---|
| ***Source:*** | Work Package C8;   R-C8A-002y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R229** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of provided service levels and data governance practices. |
| ***Cloud Actors:*** | Cloud provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C8;   R-C8A-003y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R230** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to legislative regimes without exposing security vulnerabilities. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Liability |
| ***Source:*** | Work Package C8;   R-C8A-004y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R231** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to legislative regimes for specific industry or public sectors. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Liability |
| ***Source:*** | Work Package C8;   R-C8A-005y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R232** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with competition laws (non-cooperation) in the provision of services. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Liability |
| ***Source:*** | Work Package C8;   R-C8A-006y |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R233** |
|---|---|
| ***Requirement:*** | The Cloud Provider shall provide evidence of compliance with respect to extraterritorial legislative regimes. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Liability |
| ***Source:*** | Work Package C8;   R-C8A-007y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R234** |
| ***Requirement:*** | The Cloud Provider shall provide evidence that revoked consent has been acted on in a reasonable manner. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Responsiveness |
| ***Source:*** | Work Package C8; R-C8A-008y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R235** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of who has the authority to investigate any policy compliance. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Auditor, Cloud Supervisory Authority |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability, Liability |
| ***Source:*** | Work Package C8; R-C8A-009y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R236** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of data gathered, inferred or aggregated. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C8; R-C8A-010y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R237** |
| ***Requirement:*** | The Cloud Customer (Cloud Subject) shall know, if and which third-party cloud providers are involved in the provision of the service used. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | Transaprency |
| ***Source:*** | Work Package C8; R-C8A-012y |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R238** |
| ***Requirement:*** | The Cloud Provider shall provide evidence of security breaches. |
| ***Cloud Actors:*** | Cloud Provider |
| ***Accountability Attributes:*** | Transparency, Responsibility, Verifiability, Attributability, Observability |
| ***Source:*** | Work Package C8; R-C8A-013y |
| ***Rationale:*** | |

## Appendix E. Requirements for Accountability Mechanisms

This section lists requirements for specific accountability mechanisms, in particular software tools.

### Elicited Requirements for the Cloud Offering Advisory Tool (COAT)

| | |
|---|---|
| ***Requirement ID #:*** | **R239** |
| ***Requirement:*** | COAT shall consider the needs of large corporations and organisations. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-052z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R240** |
| ***Requirement:*** | COAT shall address changes in legal requirements and best practices quickly; it shall be dynamic in nature instead of a static library of options and correct answers. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | Liability |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-053z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R241** |
| ***Requirement:*** | COAT shall be independent and with no hidden criteria for showing one cloud provider on top of the list, other than the explicit ones. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-054z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R242** |
| ***Requirement:*** | COAT shall allow the tool user to select criteria of the required services, without asking for any specific offer or cloud provider. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-055z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R243** |
| ***Requirement:*** | COAT shall support a verification process behind the procedure for adding a cloud provider to the list of providers of the tool. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-056z |
| ***Rationale:*** | One possibility is some crowd sourcing in that people who trust a certain provider can add response in some way. |

| | |
|---|---|
| ***Requirement ID #:*** | **R244** |
| ***Requirement:*** | COAT shall support a procedure of updating prices of the cloud offerings in order to assure that the prices showed for each cloud provider are the actual prices. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-057z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R245** |
| ***Requirement:*** | COAT shall have a simple organisation of the and easy to find offering selection criteria. Tool users shall be able to add and recommend new criteria (based on a sound characterisations of cloud offerings). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-058z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R246** |
| ***Requirement:*** | COAT shall support selection criteria based on what tool users need (and not only on what offered by providers). |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-059z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R247** |
| ***Requirement:*** | COAT shall allow the Cloud Provider to adjust and update offerings to new emerging criteria. COAT shall allow existing cloud providers to identify other providers that match similar criteria. The Cloud Customer who has used a specific cloud provider can give ratings, about hoe the provider is trusted. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-060z |
| ***Rationale:*** | Trend analysis is a classical mechanism for understand the market. |

| | |
|---|---|
| ***Requirement ID #:*** | **R248** |
| ***Requirement:*** | COAT shall provide a history of the incidents and how they were addressed by the involved providers. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-061z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R249** |
| ***Requirement:*** | COAT shall address the needs of cloud customers who seek cloud providers but are uncertain about what to look for. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-062z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R250** |
| ***Requirement:*** | COAT shall provide a validation of maturity, economic liability and other business operational criteria of the providers. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-063z |
| ***Rationale:*** | |

### Elicited Requirements for the Data Track Tool

| | |
|---|---|
| ***Requirement ID #:*** | **R251** |
| ***Requirement:*** | The Data Track Tool shall have a very secure system to protect all the data that is collected about services (for example, data base should be encrypted). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-029z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R252** |
| ***Requirement:*** | The Data Track Tool shall help Cloud Subjects to delete the data they do not want to have spread on the Cloud Providers (e.g. direct link, set of steps, guidelines, etc.). |
| ***Cloud Actors:*** | Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-030z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R253** |
| ***Requirement:*** | The Data Track shall help finding the policies from each Cloud Provider. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-031z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R254** |
| ***Requirement:*** | The Data Track Tool shall help users proactively by warning them about both explicit and implicit data that providers collects about users, so I can act before user submit data. |
| ***Cloud Actors:*** | |

| | |
|---|---|
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-032z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R255** |
| ***Requirement:*** | The Data Track Tool shall allow user to classify data in different levels of sensitiveness and also different classes of data (e.g. banking data, health data and other personal data). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-033z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R256** |
| ***Requirement:*** | The Data Track Tool shall allow classification and prioritization of data. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-034z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R257** |
| ***Requirement:*** | The Data Track Tool shall have an option of not only seeing which information is everywhere, but also if I want to change an information, then change in all services (e.g., the cloud subject changes the home address and now wants to update this information in all services holding this information). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-035z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R258** |
| ***Requirement:*** | The Data Track Tool shall have an option of SHARE information with other services or other cloud subjects, and track with whom the information was shared. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-036z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R259** |
| ***Requirement:*** | The Data Track Tool shall have a status of how safe a cloud subject is based on the data from cloud providers. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-037z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R260** |
| ***Requirement:*** | The Data Track Tool shall have different profiles of data information, so that the cloud subject can see data from different selective viewpoints. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-038z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R261** |
| ***Requirement:*** | The Data Track Tool shall have a guide to how to delete data in different cloud providers or a link to the where the provider explains how to delete data from the specific cloud provider. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Provider |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-039z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R262** |
| ***Requirement:*** | The Data Track Tool, in case of deletion of information, shall show whether the information has been already deleted completely by cloud providers (or just simply made unavailable but still stored by services). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-040z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R263** |
| ***Requirement:*** | The Data Track Tool shall have a weekly, monthly or annually 'warning message' of what the safe level of data is. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-041z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R264** |
| ***Requirement:*** | The Data Track Tool shall show the level of security of certain types of data that the cloud subject is concerned with. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-042z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R265** |
| ***Requirement:*** | The Data Track Tool shall give a 'warning message' when privacy rules change on cloud services, and which data are affected by the change of the rules. |

| | |
|---|---|
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-043z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R266** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall inform about privacy changes or any other changes of the cloud provider. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-044z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R267** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall help tracking different types of data format such as videos and photos. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-045z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R268** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall be deployed as a locally installed tool (not a cloud or internet service). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-046z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R269** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall show explicitly in which country data are stored or can be stored. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-047z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R270** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall show explicitly what data access has the country (local) government of where data are stored. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-048z |
| ***Rationale:*** | |

| ***Requirement ID #:*** | **R271** |
|---|---|
| ***Requirement:*** | The Data Track Tool shall be tested in different data contexts or application domains (e.g. health data, financial data, personal data). |

| | |
|---|---|
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-049z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R272** |
| ***Requirement:*** | The Data Track Tool shall be usable by people that have no or little familiarity with personal computers (PCs). |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3;  R-B2C-050z |
| ***Rationale:*** | |

| | |
|---|---|
| ***Requirement ID #:*** | **R273** |
| ***Requirement:*** | The Data Track Tool shall be usable by older people as well as young people. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Stakeholder Workshop WS3; R-B2C-051z |
| ***Rationale:*** | |

# Appendix F. Requirements for Policy Languages Tailored to Accountability

| | |
|---|---|
| ***Requirement ID #:*** | **R274** |
| ***Requirement:*** | The policy language shall allow the Cloud Customer (Cloud Subject) to express preferences about the usage of personal and sensitive data. In particular, the Cloud Subject shall be able to specify how personal data is to be processed, to whom data can be released and under which conditions. |
| ***Cloud Actors:*** | Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Capturing privacy preferences |

| | |
|---|---|
| ***Requirement ID #:*** | **R275** |
| ***Requirement:*** | The policy language shall allow anonymous or pseudonymous access control. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Anonymity/Pseudonymity |

| | |
|---|---|
| ***Requirement ID #:*** | **R276** |
| ***Requirement:*** | The policy language shall enable the personal data minimization principle as an optional requirement. The Cloud Provider and the Cloud Customer shall limit the collection of personal data to what is directly relevant and necessary to enforce a given security policy. |
| ***Cloud Actors:*** | Cloud Provider, Cloud Customer, Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Data minimization |

| | |
|---|---|
| ***Requirement ID #:*** | **R277** |
| ***Requirement:*** | Attaching policies to data shall be considered in the design of the policy language. The language shall provide mechanisms to identify what the Cloud Subject allows regardless whoever transmits the data. |
| ***Cloud Actors:*** | Cloud Subject |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Strong Policy binding |

| | |
|---|---|
| ***Requirement ID #:*** | **R278** |
| ***Requirement:*** | The policy language shall be able to express rules about data retention. It shall be possible to express the retention time but also additional metadata information. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Appropriateness, Effectiveness, Transparency |

| | |
|---|---|
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Data retention |

| ***Requirement ID #:*** | **R279** |
|---|---|
| ***Requirement:*** | The policy language shall be able to express legal policies. It shall provide the constructs to express the regulatory constructs in a machine-readable format. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Expressing regulatory constraints |

| ***Requirement ID #:*** | **R280** |
|---|---|
| ***Requirement:*** | The policy language shall be able to capture access control policies |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Access control |

| ***Requirement ID #:*** | **R281** |
|---|---|
| ***Requirement:*** | The policy language shall provide delegation capabilities so that the administration and the management of authorization decisions can be decentralised and distributed to third parties. The policy language shall allow expressing which rights are delegated. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Delegation of rights |

| ***Requirement ID #:*** | **R282** |
|---|---|
| ***Requirement:*** | The policy language shall describe the clauses in a way that actions taken upon enforcing the policy can be audited. The policy language shall support ways to define what types of operations need to be audited and for which purposes. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Auditability |

| ***Requirement ID #:*** | **R283** |
|---|---|
| ***Requirement:*** | The policy language shall indicate which conditions in access control policy shall be revealed. Each condition in the policy can be subject to a disclosure policy. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Controlling policy disclosure |

| ***Requirement ID #:*** | **R284** |
|---|---|
| ***Requirement:*** | The policy language shall offer a way to send notifications to the Cloud Subject and third parties in case of policy violations or other incidents. |
| ***Cloud Actors:*** | Cloud Subject, Cloud Customer |
| ***Accountability Attributes:*** | Transparency, Responsiveness, Remediability |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Reporting and notification |

| ***Requirement ID #:*** | **R285** |
|---|---|
| ***Requirement:*** | The policy language shall enable recommendations for redress in the policy in order to set right what was wrong and what made a failure occur. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Verifiability, Attributability, Observability, Responsiveness, Remediability |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Redress |

| ***Requirement ID #:*** | **R286** |
|---|---|
| ***Requirement:*** | The policy language shall allow revoking granted access and an authorised usage to a resource. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Responsiveness, Remediability |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Revocability |

| ***Requirement ID #:*** | **R287** |
|---|---|
| ***Requirement:*** | The policy language shall specify which events have to be logged and what information related to the logged event have to be added to the log. The policy language shall express the way the information is logged (e.g. how, when, where, etc.). |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Logging |

| ***Requirement ID #:*** | **R288** |
|---|---|
| ***Requirement:*** | The policy language shall be able to express rules about data localization such that accountable services can signal where the data centres hosting them are located. Policies shall also be able to accommodate future demands concerning upcoming regulations that frame international data transfers and extra-territorial laws which may require different levels of transparency towards different cloud actors. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | Transparency, Liability |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |

| | |
|---|---|
| ***Rationale:*** | Controlling data location and transfer |

| | |
|---|---|
| ***Requirement ID #:*** | **R289** |
| ***Requirement:*** | The policy language shall be able to express usage control rules. |
| ***Cloud Actors:*** | |
| ***Accountability Attributes:*** | |
| ***Source:*** | Work Package C4 Policy Language; R-C4A-001z |
| ***Rationale:*** | Usage control rules |

## Appendix G. Flow of requirements in A4Cloud

A4Cloud is a complex project with many work packages creating and consuming requirements. These work packages are connected in many ways; however, the DoW does not describe in full detail how all work packages cooperate. This section describes the flow of requirements in A4Cloud as can be interpreted from the Description of Work (DoW). We show which work packages that create requirement artefacts (internal or external deliverables and other kinds of files that concern requirements), and in which work packages these artefacts are used. It is essential to understand who will use the requirements. By understanding the context in which the requirements will be applied (i.e. who needs them for what) it will be possible to understand how to manage the requirements.

Furthermore, work packages involved in requirements work have several requirement activities in addition to internal and external deliverables. Therefore it is difficult to get a full overview of the flow of requirements in the project. However, this knowledge is essential when it comes to tracking requirements. Several questions emerge: Which work packages and which activities create requirements? Through which artefacts are these requirements conveyed to other parts of the A4Cloud work? Who will need them, and when? Which stakeholders will be involved in identifying requirements? How do we handle dependences and conflicts between requirements? Do we describe them in one common way? How do we make certain that the last version of a requirement is communicated to the receiving work packages?

Motivated by these questions we decided to study the gathering and use of A4Cloud requirements. We have performed this work in several stages. First we analysed the DoW as it describes in detail what each work package will create and what the work package communicates to other parts of the project. We looked for specific details on the creation of requirements artefacts and tracked their flow. At the A4Cloud General meeting on March 2013 in Malaga,, a list was created that in detail shows the relationship between each work package currently in operation at that time. Second, we created a requirement flow figure, which described each work package down to the level of individual tasks and requirement artefacts (i.e. project internal milestone report such as MS:C-4.1 and public deliverables such as D:B-4.2 [8]). We also noted the month each artefact is supposed to be delivered. Third, we asked for input from everyone involved in the project, and we approached every work package leader directly asking to review the flow diagram. Finally, we updated the figure shown in Figure 9**Error! Reference source not found.**.

Most requirements artefacts are only used by one or two other tasks. Also, streams B and C seem to produce approximately the same number of requirement artefacts (documents in some way containing requirements). Stream D is the one that probably will need the requirements the most (from the reply from the WP leaders), however this is not shown in the figure, because there is not a formal link to them at the DoW.

Since all requirements seem to come from one task and then go directly to another task, one way of coordinating requirements will be by updating this map. Then everyone that produce or use requirements can use this map to get an overview of who will use them and for what purpose. Requirements will also be documented in specific artefacts. Since requirements will be updated and changed, it is important that everyone knows where to find the latest version. The same requirements must not be documented in several places; this is where the requirements repository comes in (see Appendix C).

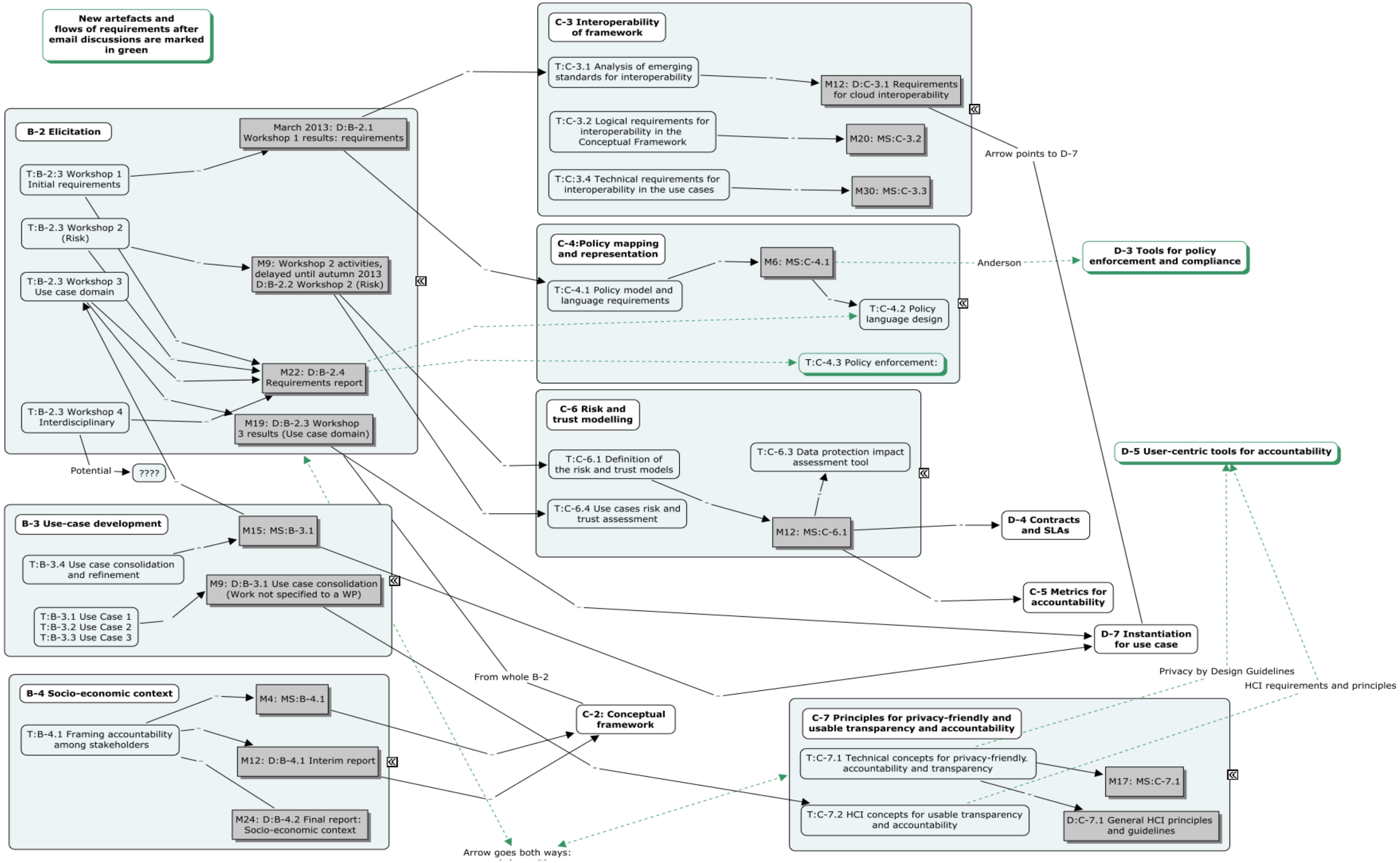

New artefacts and flows of requirements after email discussions are marked in green
B-2 Elicitation
March 2013: D:B-2.1 Workshop 1 results: requirements
T:B-2:3 Workshop 1 Initial requirements
T:B-2.3 Workshop 2 (Risk)
M9: Workshop 2 activities, delayed until autumn 2013 D:B-2.2 Workshop 2 (Risk)
T:B-2.3 Workshop 3 Use case domain
M22: D:B-2.4 Requirements report
T:B-2.3 Workshop 4 Interdisciplinary
M19: D:B-2.3 Workshop 3 results (Use case domain)
Potential
????
B-3 Use-case development
M15: MS:B-3.1
T:B-3.4 Use case consolidation and refinement
M9: D:B-3.1 Use case consolidation (Work not specified to a WP)
T:B-3.1 Use Case 1
T:B-3.2 Use Case 2
T:B-3.3 Use Case 3
B-4 Socio-economic context
M4: MS:B-4.1
T:B-4.1 Framing accountability among stakeholders
M12: D:B-4.1 Interim report
M24: D:B-4.2 Final report: Socio-economic context
C-3 Interoperability of framework
T:C-3.1 Analysis of emerging standards for interoperability
M12: D:C-3.1 Requirements for cloud interoperability
T:C-3.2 Logical requirements for interoperability in the Conceptual Framework
M20: MS:C-3.2
T:C:3.4 Technical requirements for interoperability in the use cases
M30: MS:C-3.3
Arrow points to D-7
C-4:Policy mapping and representation
M6: MS:C-4.1
Anderson
D-3 Tools for policy enforcement and compliance
T:C-4.1 Policy model and language requirements
T:C-4.2 Policy language design
T:C-4.3 Policy enforcement:
C-6 Risk and trust modelling
T:C-6.3 Data protection impact assessment tool
T:C-6.1 Definition of the risk and trust models
T:C-6.4 Use cases risk and trust assessment
M12: MS:C-6.1
D-4 Contracts and SLAs
C-5 Metrics for accountability
D-5 User-centric tools for accountability
D-7 Instantiation for use case
From whole B-2
C-2: Conceptual framework
Privacy by Design Guidelines
HCI requirements and principles
C-7 Principles for privacy-friendly and usable transparency and accountability
T:C-7.1 Technical concepts for privacy-friendly accountability and transparency
M17: MS:C-7.1
T:C-7.2 HCI concepts for usable transparency and accountability
D:C-7.1 General HCI principles and guidelines
Arrow goes both ways:

**Figure 9: A4Cloud flow of requirements as deduced from the DoW.**