
D:B-3.1 Use Case Descriptions

Deliverable Number: D23.1

Work Package: WP 23

Version: Final

Deliverable Lead Organisation: SINTEF

Dissemination Level: PU

Contractual Date of Delivery (release): 30th June, 2013

Date of Delivery: 27th June, 2013

Editor

Karin Bernsmed (**SINTEF**)

Contributors

Karin Bernsmed (SINTEF), Massimo Felici (HP Labs), Anderson Santana De Oliveira (SAP), Jakub Sendor (SAP), Nils Brede Moe (SINTEF), Thomas Rübsamen (Furtwangen), Vasilis Tountopoulos (ATC), Bushra Hasnain (QMUL)

Table of Contents

- List of Figures5
- List of Tables5
- Abbreviations6
- Executive Summary.....7
- 1 Introduction8
 - 1.1 Relationship to Other A4Cloud Work Packages and Deliverables8
 - 1.2 Relation to the DoW.....9
 - 1.3 Outline9
- 2 Cloud Ecosystems10
 - 2.1 Reference Architecture and Taxonomy 10
 - 2.2 Cloud Usage Scenarios 11
 - 2.3 Chains of Accountability 13
 - 2.4 Controllers, Processors and Data Subjects in Cloud Ecosystems 14
- 3 Business Use Case Definition and Approach16
- 4 Business Use Cases.....18
 - 4.1 BUC 1: Health Care Services in the Cloud 18
 - 4.1.1 Overview 18
 - 4.1.2 Cloud Actors..... 19
 - 4.1.3 Emerging Issues in the Cloud Ecosystem 19
 - 4.1.4 Usage scenarios 22
 - 4.2 BUC 2: Cloud-based ERP Software Enabled with Third Party Extensions 23
 - 4.2.1 Overview 23
 - 4.2.2 Cloud Actors..... 24
 - 4.2.3 Emerging Issues in the Cloud Ecosystem 25
 - 4.2.4 Usage Scenarios..... 26
 - 4.3 BUC 3: Rights and Relevant Obligations in a Multi-tenant Cloud 26
 - 4.3.1 Overview 26
 - 4.3.2 Cloud Actors..... 27
 - 4.3.3 Emerging Issues in the Cloud Ecosystem 28
 - 4.3.4 Usage Scenarios..... 29
- 5 Scenarios30
 - 5.1 The Role of Scenarios in A4Cloud..... 30
 - 5.2 Developing Scenarios..... 30

D:B-3.1 Use Case Descriptions

- 5.3 Guidelines for Creating a Scenario 31
- 6 Accountability Relationships in the Business Use Cases 32
 - 6.1 Accountability relationships in Business Use Case 1 33
 - 6.2 Accountability relationships in Business Use Case 2 35
 - 6.3 Accountability relationships in Business Use Case 3: 36
- 7 High-level Functional Analysis of the To-be Scenarios 38
 - 7.1 Functionalities for individual end users (cloud users) 38
 - 7.2 Functionalities for business end users (cloud users) 39
 - 7.3 Functionalities for cloud providers 41
 - 7.4 Functionalities for cloud auditors 43
- 8 Conclusions 45
- References 46
- Appendix A An A4Cloud Taxonomy of Stakeholders 47
- Appendix B Data Controllers and Processors 48
- Appendix C Scenarios for Business Use Case 1 49
 - Scenario 1: Kim 49
 - Scenario 2: Sandra 51
 - Scenario 3: Michael 52
 - Scenario 4: Peter 54
 - Scenario 5: Bruce 55
 - Scenario 6: Leslie 56
- Appendix D Scenarios for Business Use Case 2 57
 - Scenario 7: Alice 57
 - Scenario 8: Bob 58
 - Scenario 9: Charles 59
 - Scenario 10: David 60
 - Scenario 11: Edgar 60
 - Scenario 12: Frank 61
- Appendix E Scenarios for Business Use Case 3 62

D:B-3.1 Use Case Descriptions

Scenario 13: Sandra 62

Scenario 14: Paul 63

Scenario 15: Roger 64

Scenario 16: Michael..... 65

Scenario 17: John 65

Scenario 19: Linda 67

Scenario 20: Peter 67

List of Figures

Figure 1 Examples of cloud computing usage scenarios (drawn from [10])	12
Figure 2 Context of accountability support for the cloud	13
Figure 3 The MedNet platform.....	20
Figure 4 Actors involved in the ERP business use case	24
Figure 5 Cloud ecosystem for the multi-tenancy business use case	27
Figure 6 The relation between as-is scenarios, to-be scenarios and UML use cases.....	30
Figure 7 The role of the accountability attributes in the interactions between actors	33
Figure 8 An A4Cloud taxonomy of stakeholders	47
Figure 9 Controllers and processors under the Directive 95/46/EC	48
Figure 10 Confidential and personal data flows	62
Figure 11 Business and personal data flows.....	66

List of Tables

Table 1 The accountability relationships between the actors involved in BUC1	34
Table 2 The accountability relationships between the actors involved in BUC2	36
Table 3 The accountability relationships between the actors involved in BUC3	37
Table 4 Functionalities for individual end users (cloud users)	38
Table 5 Functionalities for business end users (cloud users)	40
Table 6 Functionalities for cloud providers	41
Table 7 Functionalities for cloud auditors	43

Abbreviations

A4Cloud	Accountability For Cloud and Other Future Internet Services
AAL	Ambien Assistant Living
BUC	Business Use Case
BYOD	Bring Your Own Device
DoW	Description of Work
EU	European Union
ERP	Enterprise Resource Planning
GP	General Practitioner
IaaS	Infrastructure as a Service
ISV	Independent Software Vendors
PaaS	Platform as a Service
PSP	Primary Service Provider
SaaS	Software as a Service
UML	Unified Modelling Language
WP	Work Package

Executive Summary

This deliverable describes the different business use cases that will be investigated in the A4Cloud project. They are all examples of services that will benefit strongly from being realized as cloud services but that will have stringent requirements for accountability and transparency in the cloud service provision chain. A4Cloud contributes toward an accountability-based approach enabling different mechanisms and tools that help cloud users, 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 selected business use cases demonstrate how these accountability mechanisms and tools can be applied in three distinct domains, all involving the generation, storage and processing of personal and business confidential data by different actors in cloud ecosystems. This deliverable describes the three business use cases:

- **Business use case 1** deals with the flow of healthcare information generated by medical sensors in the cloud. It focuses on the generation, processing, flow and traceability of sensitive personal information between a set of cloud providers. The case shows which accountability mechanisms and tools that will be needed to protect sensitive personal data.
- **Business use case 2** deals with cloud-based Enterprise Resource Planning (ERP) software, which is extended with third party services. The purpose is to show how an enterprise cloud deployment that originally has been configured as an on-premises system can be extended with new capabilities by combining it with service extensions running in the cloud. This business use case demonstrates how personal information originating from end users can be adequately protected across a chain of cloud service models (IaaS, PaaS, and SaaS), using accountability mechanisms and tools.
- **Business use case 3** deals with a multi-tenant cloud scenario. This business use case is concerned with challenges that arise when end users operate with cloud services for personal as well as business purposes on the same device. It shows how accountability mechanisms and tools can help solve the intersection of policy enforcements across different cloud domains. In contrast to business use case 2, which illustrates service chains in one domain, this business use case comprises multi-tenant service chains of different domains.

This deliverable gives a brief introduction to each case, outlines how the business use cases relate to the A4Cloud conceptual framework and shows how they complement each other in terms of different requirements for accountability in the cloud. A description of the business use cases in terms of to-be scenarios highlights the need for and use of accountability mechanisms and tools in different cloud application domains. Finally, it provides a high-level functional analysis of the scenarios, which shows what functionalities that are used by the different personas described in the to-be scenarios. These functionalities will further feed the related work packages with functional requirements that should be met in the implementation of the A4Cloud preventive, detective and corrective mechanisms and tools.

1 Introduction

The A4Cloud project deals with accountability for the cloud and other future Internet services. In the context of the project, accountability concerns data stewardship regimes in which organizations that are entrusted with personal and business confidential data are responsible and liable for processing, sharing, storing and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties) [1]. A4Cloud contributes toward an accountability-based approach by enabling different mechanisms and tools for how personal and business confidential information is managed in the cloud, taking into account the chain of responsibilities that needs to be built throughout the cloud service supply network.

This deliverable describes three business use cases that motivate the need for and that demonstrate the use of the A4Cloud accountability-based approach. The business use cases represent real-life examples of cloud services that would benefit from clear accountability relationships (in terms of responsibility, transparency and liability) between different actors in cloud ecosystems. This deliverable presents the business use cases in terms of “as-is” and “to-be” scenarios (textual descriptions). The consolidated report (Deliverable D:B-3.2 Consolidated use case report, which will be delivered in September 2014) will model aspects of the business use cases by different diagrammatic notations (e.g. UML use case diagrams). The main purpose of this deliverable is to show how the different business use cases reflect the scope of the A4Cloud project, and to serve as input to the research and development work done in the rest of the project.

1.1 Relationship to Other A4Cloud Work Packages and Deliverables

This deliverable is related to a number of other work packages in A4Cloud project. Here we list the most important relations.

- The goal of the **WP:B-2 (elicitation)** work package is to ensure that the project activities reflect the needs of stakeholder groups. This is achieved through the organisation of stakeholder workshops, which aim 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. WP:B-2 relies on input from WP:B-3 in order to make the requirements elicitation part of the first workshop more concrete to the stakeholders. We have therefore provided high-level descriptions of all three business use cases to WP:B-2. In return, WP:B-2 has provided WP:B-3 with detailed feedback on the business use cases; in particular on the relevance of the scenarios and on what accountability properties that the stakeholder believe is desired in the different domains. In the next round, functional requirements on a user level (the UML use case diagrams) will be provided as input to WP:B-3.
- The goal of the **WP:B-5 (contractual & regulatory considerations)** work package is (amongst other things) to assess the legal responsibilities and regulatory implications for the different actors in the cloud ecosystem in the context of the project. WP:B-5 has provided feedback to the business use case description and scenarios in this deliverable, in terms of an analysis of emerging accountability issues in the different domains and input on the different actors' responsibilities in accordance with the legislation.
- The goal of the **WP:C-2 (conceptual framework)** work package is to identify and describe a framework of concepts that forms the basis for the accountability mechanisms and tools that will be developed in the project. This work package will use these concepts when describing, modelling and analysing the business use cases. Through WP:B-3, WP:C-2 will receive requirements originating from the business use cases.
- The goal of the **WP:C-4 (policy mapping and representation)** work package is to define a framework for enforceable accountability policies. The framework will be validated by modelling the business use cases documented in this deliverable. To do this, WP:C-4 will translate the regulations, contracts and privacy policies the business use cases must comply with into the defined policy language.
- The goal of the **WP:C-6 (risk and trust modelling)** work package is to provide abstract models of risk and trust amongst the cloud stakeholders, and to create representations of these concepts. The risk and trust models will be validated by modelling the business use cases that have been defined in this deliverable.

D:B-3.1 Use Case Descriptions

- The goal of the **WP:C-7 (Principles for transparency and accountability)** work package is to elaborate design principles for the transparency and accountability tools that will be developed in A4Cloud. This work package will (amongst other things) develop design principles for interfaces addressing the to-be scenarios outlined in this deliverable. WP:C-7 is also analysing the privacy risks of the A4Cloud tools in relation to the business use cases.
- The goal of the **WP:D-7 (instantiation for use cases)** work package is to enable demonstration and evaluation of use of the business use cases. The business use cases that will be developed in WP:B-3 will serve as input to this work.

In addition, this deliverable is closely related to several other documents that have been produced in the A4Cloud project.

- The terminology and concepts outlined in the A4Cloud milestone document **MSC-2.1 Scoping report and initial glossary** [2] have been used consistently throughout this deliverable.
- The A4Cloud deliverable **D:B-2.1 Stakeholder Workshop 1 Results (Initial Requirements)** [3] has served as the main source for eliciting business use cases characteristics that reflect the concerns of real cloud stakeholders.

1.2 Relation to the DoW

The A4Cloud Description of Work (DoW) describes the development of three different "use cases" which are representations of real world situations in three distinct user domains. These are instances of scenario-based development covering several types of cloud actors and their interactions with the A4Cloud tools and technologies. However, the term "use case" is often used by engineers and system designers to refer to a technique that can be used to capture the functional requirements of a system [4]. To avoid confusion we have therefore chosen to use the term "business use cases" rather than "use cases" in this document when referring to the high level representations of the real world situations. When we use the term "UML use case" later on in this document, it is the requirements capturing technique that we refer to. The UML use cases will be presented in the next WP:B-3 deliverable (D:B-3.2).

The A4Cloud DoW outlines three different business use cases. The first, which is led by SINTEF, is related to healthcare and describes a case where sensitive personal information originating from a set of body sensors will flow through a set of cloud providers. However, the A4Cloud DoW outlines an example which concerns the protection of personal health records that is transferred between different organizations, different organizational domains and across national borders in the European Union. The reason for why we have chosen to slightly change the focus of this business use case, is to align it with the current strategy and research interests of our network of stakeholders in the healthcare domain.

1.3 Outline

The deliverable is structured as follows. This section introduces the overall approach that has been followed in WP:B-3 and explains its relation to the other work packages in the project and to the DoW. Section 2 explains the cloud ecosystem with its main actors and the roles they are taking, and provides some high-level usage scenarios illustrating the usage of cloud services. This section also briefly discusses the roles of data controllers, data processors and data subjects in cloud ecosystems. Section 3 outlines the business use case definition and approach taken. Section 4 then analyses the business use cases, in terms of the system that is to be considered, the actors involved and their means of accountability. In Section 5 we introduce the scenarios (which are detailed in Appendices C-E). Section 6 describes the accountability relationship in the business use cases and Section 7 summarizes what functionalities that will be needed to achieve accountability in the to-be scenarios. Finally, Section 8 provides our main conclusion and an outlook to future work.

2 Cloud Ecosystems

The NIST definition of cloud computing [1] identifies the essential characteristics of a cloud (i.e. on-demand, self-service, broad network access, resource pooling, rapid elasticity and measured services), the service models (i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) and deployment models (i.e. private, community, hybrid and public clouds). According to the NIST definition “*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*”. The combination of such cloud computing features enables different business models; hence, cloud ecosystems involve various stakeholders, for example cloud users and cloud providers. This section briefly describes the NIST cloud computing reference architecture, in terms of different cloud services and roles. The NIST reference architecture forms the basis for our taxonomy of stakeholders that has been used in this work package to harmonise and standardise the descriptions of the business use cases. We also provide some sample usage scenarios that illustrate basic interactions with cloud services in order to explain cloud ecosystems. In order to stress the relevance of the business use cases, this section stresses the need for chains of accountability (as described in MS:C-2.2 Initial conceptual framework [5]) in cloud ecosystems. Finally, we provide a brief analysis of the current data protection directive (Directive 95/46/EC [6]), which highlights the distinction between data controllers and data processors. This distinction is necessary in order to systematically assign specific roles to actors in cloud ecosystems according to relevant regulatory directives. We are then able to describe cloud ecosystems according to cloud computing definitions as well as to definitions drawn from the relevant data protection directives.

2.1 Reference Architecture and Taxonomy

The NIST cloud computing reference architecture [7] identifies the main actors and roles in a cloud ecosystem, their activities and functions in terms of cloud computing. The terminology used in this deliverable is based on the identified roles in [7] to describe consistently the cloud ecosystems of the three business use cases. We have identified five main cloud actors:

- **Cloud user¹:** A cloud user is a person or an organization that maintains a business relationship with, and uses service from, one or more cloud providers. Cloud users who are persons are denoted **individual end users** in this deliverable, whereas cloud users who are organisations are denoted **business end users**.
- **Cloud provider:** A cloud provider is a person, organization, or entity responsible for making a cloud service available to interested parties. Note that an entity can be both a cloud user and a cloud provider (e.g., in a service provision chain).
- **Cloud auditor²:** A cloud auditor is a party that can conduct independent assessments of cloud services, information system operations, performance and security of the cloud implementation,
- **Cloud broker:** A cloud broker is an entity that manages the use, performance and delivery of cloud services, and/or negotiates relationships between cloud providers and cloud users.
- **Cloud carrier:** A cloud carrier is an intermediary that provides connectivity and transport of cloud services from cloud providers to cloud users.

¹ The NIST taxonomy uses the term *cloud consumer* rather than cloud user. In the A4Cloud project, the terms “cloud user” and “cloud consumer” have so far been used interchangeably. In order to avoid different understandings of the terms, in particular with the more general and business notion of consumer, this deliverable consistently uses the term “cloud user” to identify any individual or organisation having access to a cloud service provided by a third party. Moreover, this simplifies the alignment of the terminology with the data protection directive, in particular, with the terms of data subjects, data controller and data processor.

² Note that additional roles could be added (although they are not central for the scope of this project and the business use cases) such as, for instance, law enforcement actors. This would extend the categorization given by NIST, in order to cover governance by identifying other actors that currently fit under “cloud auditor”.

D:B-3.1 Use Case Descriptions

Taxonomies may be used to structure the analysis of interactions and responsibilities among cloud actors in a systematic manner, in order to identify contingencies [8]. Moreover, they allow us to describe cloud ecosystems and to map actors to specific roles and responsibilities. By identifying roles and responsibilities in cloud ecosystems we can analyse relationships and dependencies between cloud services (and software) in order to understand emerging risks (e.g. security and privacy risks) [8]. The roles defined by NIST are part of a cloud taxonomy, which consists of four different levels of abstraction [7]:

- **Level 1: Role**, which indicates a set of obligations and behaviours as conceptualized by the associated actors in the context of cloud computing.
- **Level 2: Activity**, which entails the general behaviours or tasks associated to a specific role.
- **Level 3: Component**, which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity.
- **Level 4: Sub-component**, which present a modular part of a component.

The four-level taxonomy identifies the main concepts underpinning the NIST reference architecture for cloud computing presented in [7]. Figure 8 in Appendix A shows the A4Cloud taxonomy of stakeholders that has been developed in this project. This taxonomy combines different viewpoints of analyses and highlights how A4Cloud extends the cloud computing taxonomy developed by NIST with an accountability perspective. That is, accountability (and its main elements or means to achieve accountability) will be considered as the principal conceptual viewpoint in order to analyse relationships among different roles in cloud ecosystems. Such analyses will result in extending and detailing cloud computing taxonomies by accountability and actors (associated with specific roles) identified in cloud ecosystems. Moreover, it will allow us to identify relevant stakeholders and communities (e.g. standardization bodies, regulators) who might affect the overall applicability and relevance of A4Cloud's business use cases. At the time of writing, the A4Cloud taxonomy presented in Figure 8 has been used both to describe the business use cases in this deliverable and to organize the requirements elicitation efforts in WP:B-2.

2.2 Cloud Usage Scenarios

This section intends to support a discussion of accountability aspects of cloud computing by presenting some simple usage scenarios. The NIST recommendations use the different cloud actors in order to discuss usage scenarios with respect to a conceptual reference model [9]. The different usage scenarios described in [10] capture different cloud deployments. Here different high-level generic scenarios are analysed in different deployment dimensions (i.e. one/multiple cloud domains, within/outside trusted boundaries). Depending on the deployment models (i.e. private, community, public and hybrid), cloud providers and users interact differently. Their (security) perimeters (or boundaries) would define control and visibility over deployed resources. Hence, they experience the cloud from different perspectives. In particular, they might be exposed to different degrees of emerging issues (e.g. network dependency, risks from multi-tenancy, performance limitations, etc.) in the cloud.

A4Cloud enhances cloud deployments by accountability relationships. That is, the NIST recommendations allow us to structure the discussion of accountability with respect to specific roles in a cloud ecosystem. The identification of specific roles (with associated responsibilities) in cloud ecosystems supports also an analysis of emerging data protection problems. The business use cases, presented in this deliverable provide sample scenarios that involve chains of accountability in cloud ecosystems. The scenarios highlight how actors in cloud ecosystems would benefit from established accountability relationships and the support given by specific accountability mechanisms and tools when dealing with data protection issues. Structured representations of the chains of accountability would allow comparison of different cloud ecosystems and identification of accountability relationships supported by A4Cloud mechanisms. The analysis of any particular cloud ecosystem should identify specific accountability relationships among actors and how they relate to the elements of accountability in high level scenarios relating to the treatment of personal data and of business confidential data within service provision chains, which are central to the interests of the A4Cloud project. The analysis of the different actors involved in any particular scenario should identify specific scenarios as well as responsibilities. Next, we describe sample scenarios that characterize cloud ecosystems. The scenarios describe interactions among cloud stakeholders who would benefit from accountability in cloud ecosystems. A number of detailed scenarios for the three different business use cases will be presented in the subsequent sections of this document.

D:B-3.1 Use Case Descriptions

Figure 1 shows some sample usage scenarios (drawn from [10]) between an end user and an enterprise interacting with a public cloud. The usage scenarios describe four simple interactions between a cloud user and a cloud provider: (1) End users accessing applications running on the cloud, (2) Employees and end users accessing applications running on the cloud, (3) Enterprise's IT integrated with cloud applications, and (4) Cloud applications on the cloud interoperating with a partner's application in a supply chain. The analysis of the usage scenarios highlights some general requirements (e.g. in terms of identity, security, Service Level Agreement (SLA), location awareness, etc.). The business use cases described in this deliverable are instances (which combine and extend such sample usage scenarios) tailored to specific application domains. Accountability provides us with an alternative perspective to analyse problems of data protection emerging in cloud ecosystems.

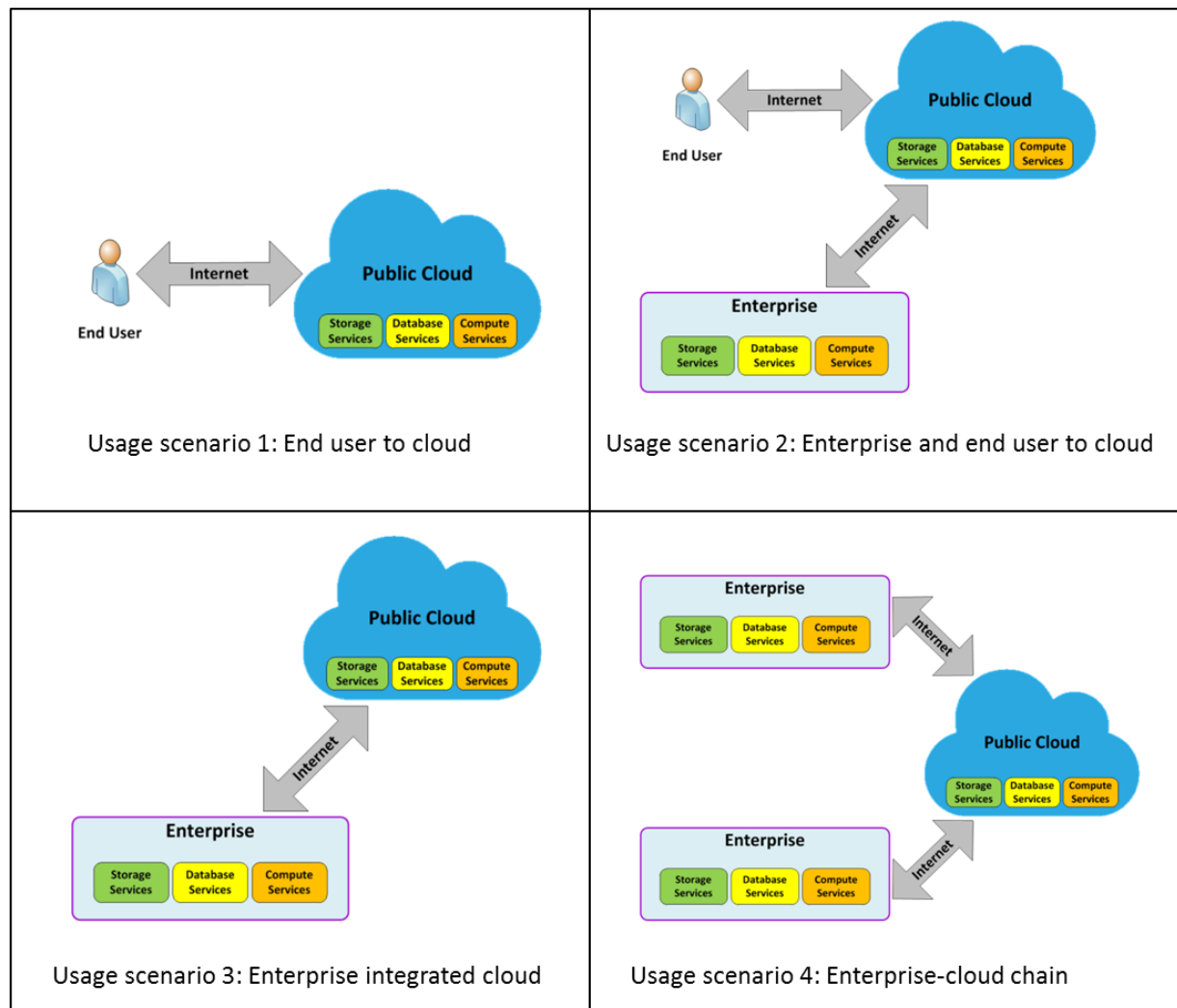


Figure 1 Examples of cloud computing usage scenarios (drawn from [10])

2.3 Chains of Accountability

This subsection highlights the relationship between the business use cases and the accountability conceptual framework, as described in the internal report MSC-2.2 [5]. In particular, it stresses how the business use cases are particular instances, hence representative, of the problem scenarios defining the scope of the A4Cloud’s accountability conceptual framework. The conceptual framework described in MSC-2.2 is based on an accountability model. The central elements of this model are: **accountability attributes**, which are the conceptual elements of accountability as used across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis), **accountability practices**, which are the emergent behaviours characterising accountable organisations (that is, how organisations operationalize accountability or put accountability into practices) and **accountability mechanisms and tools**, which are the diverse mechanisms and tools that support accountability practices (that is, accountability practices use them). This subsection explains how the A4Cloud accountability framework, based on the accountability model consisting of attributes, practices, mechanisms and tools, enables an accountability analysis of accountability relationships amongst cloud actors. The attributes of accountability (assurance, responsibility, transparency, liability, etc.) identify accountability relationships between actors. An analysis of such accountability attributes enables us to understand how accountability relationships emerge in cloud ecosystems. Figure 2 highlights how the accountability model (and the supported framework) enables cloud ecosystems.

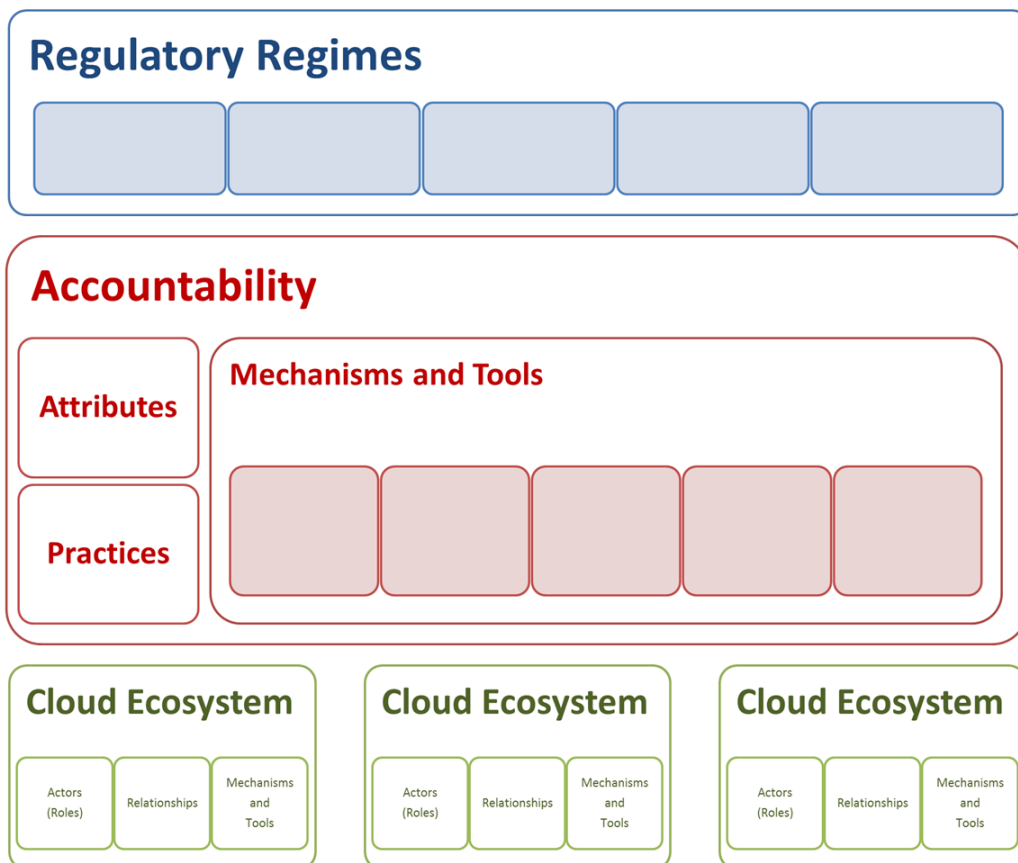


Figure 2 Context of accountability support for the cloud

The analysis of actors (roles) with respect to the accountability attributes highlights such relationships. For instance, let us consider responsibility (one of the accountability attributes) in order to analyse the relationships among actors. A cloud provider is responsible to its customers (the cloud users), as specified in the contract between them, for the way personal data is stored and maintained in the cloud. Similarly, the cloud provider is responsible to data protection authorities for complying with existing data protection legislation. The extent of the latter responsibility varies depending on the cloud provider's role in processing personal data (primarily whether the provider is a data controller or a data

processor). However, each employee of the cloud provider is responsible only to the provider, but not directly to its customers (the cloud users) and the data protection authorities. This highlights how accountability attributes enable us to analyse emerging accountability relationships among actors. Hence, different accountability relationships emerge among actors in cloud ecosystems. **Chains of accountability** consist of the set of relationships existing between any two actors in a cloud ecosystem. Analysing accountability attributes highlights emerging relationships among actors. The characterization of accountability and the analysis of these relationships in cloud ecosystems allow us to identify opportunities (in terms of mechanisms and tools) to support accountability in cloud ecosystems. Our accountability characterization of cloud ecosystems involves the identification of the main actors and the analysis of their relationships with respect to the accountability attributes.

2.4 Controllers, Processors and Data Subjects in Cloud Ecosystems

To analyse the three business use cases in terms of accountability, it is necessary to analyse the roles of the involved actors in terms of who are the *data subjects*, *data controllers* and *data processors*. The current definitions of these terms are [11]:

- **Data controller:** An entity (whether a natural or legal person, public authority, agency or other body) which alone, jointly or in common with others determines the purposes for which and the manner in which any item of personal data is processed
- **Data processor:** An entity (whether a natural or legal person, public authority, agency or any other body) which processes personal data on behalf and upon instructions of the data controller
- **Data subject:** An identified or identifiable individual to whom personal data relates, whether such identification is direct or indirect (for example, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity).

It is important to assign the roles of the involved actors correctly, since this will determine and allocate responsibilities amongst the actors. Accountability obligations arising from Directive 95/46/EC [6] are centred on the notion of *control* i.e. the entity that is perceived to have control over processing the personal data will (in most cases) be held responsible and accountable to the end user/data subject for ensuring compliance is had by all providers in the service chain. It is therefore essential that actors can be defined correctly within the roles of data controller and data processor to ensure accountability obligations are correctly imposed and owed. Figure 9 in Appendix B provides a simplified illustration of control as envisioned by Directive 95/46/EC. This figure has been used to determine whether the actors involved in the scenarios in the three different business use cases are defined as data controllers or data processors within the legislation.

The current directive on data protection (Directive 95/46/EC [6]) is being reformed and the Commission has planned to replace this legislation with the proposed draft regulation on data protection. The main principles³ relating to the processing of personal data remain conceptually the same, as do the definitions of the main actors involved in data processing; the dichotomy of controllers and processors is retained⁴. However, some changes have been proposed, which include increased responsibilities on controllers and processors, for example Article 26 clarifies the position and obligation of processors, based on Article 17(2) of Directive 95/46/EC, including that a processor who

³ Directive 95/46/EC Article 5 states that: "Personal data must be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) Adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed...

(d) Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed...

(f) Processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation."

⁴ Directive 95/46/EC Article 4

D:B-3.1 Use Case Descriptions

processes data beyond the controller's instructions is to be considered as a *joint controller*. Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC extending the obligation to processors⁵. Increased responsibilities are also introduced with reference to data subject rights in addition to more detailed chapters on data transfers and liabilities and sanctions⁶.

The proposed draft regulation on data protection is still at draft stage and going through the legislative process; the European Parliament has delayed their vote and this is now expected around September 2013. It is beyond the scope of this deliverable to consider in detail the specific changes that could come into force through the regulation. Thus the primary focus of analysis of the business use cases will be on the current data protection directive (Directive 95/46 EC). In the A4Cloud project a detailed analysis of the proposed draft regulation on data protection is being carried out under WP:B-5⁷.

⁵ Irrespective of the contract with the controller

⁶ Directive 95/46/EC Article 26, Article 17-20 and Article 73-80 respectively

⁷ See MSC:5.1 [12] and the upcoming D:B-5.1

3 Business Use Case Definition and Approach

This section outlines the business use case definitions and the approach taken to develop them.

A **business use case** provides a descriptive rationale of the use of a system at the organization level. In A4Cloud the business use cases capture the reason for why accountability is important in cloud services. The business use cases (similarly to the ones developed by NIST using a cloud computing business use case template) provide a description of example application domains that can benefit from moving to the cloud as well as from having accountability in the cloud. The three business use cases are from different business domains and are intended to show that the A4Cloud approach can span a wide space. They also reflect the different scientific and business interests of the A4Cloud partners.

This deliverable outlines three different horizontal business use cases that will be used to demonstrate how the tools and technology developed in A4Cloud can be used in three different settings. The three business use cases have been carefully chosen to complement each other in terms of which cloud actors are involved, what kind of data that is being considered and what kind of accountability relationships that arise in each domain. They all represent IT solutions for which security and privacy risks may significantly increase by moving to the cloud. The business use cases reflects the scope of what could be covered by a deployed A4Cloud framework and they will be used to demonstrate how the A4Cloud accountability approach can prevent breaches in trustworthiness, detect policy violations and correct violations that may occur. They also reflect the different scientific and business interests of the A4Cloud partners.

A **stakeholder** is someone having a legitimate interest in a project. In A4Cloud, a stakeholder means a person, group or organization that affects or can be affected by the A4Cloud project results. Figure 8 in Appendix A describes the A4Cloud taxonomy of stakeholders. All the stakeholders illustrated in this figure in in of scope for the A4Cloud project⁸.

Stakeholders are an important part of the A4Cloud project. To ensure that the project activities reflect the need of the stakeholders in the cloud ecosystem, WP:B-3 has engaged with a broad base of relevant stakeholder to elicit the business use case characteristics. This has been done through participation in the requirements elicitation efforts organised by WP:B-2, as well as through interviews and workshops with domain specific stakeholders organised locally by the partners responsible for the different business use cases. Note that even though the initial identification of suitable stakeholders was based on the A4Cloud stakeholder taxonomy (more specifically, we used the taxonomy to identify stakeholders who represented different perspectives in the cloud ecosystem and who we believed would be able to give valuable input to the project), the stakeholders that we actually interviewed were those who were available at the moment and who were willing to participate in our elicitation efforts.

A **scenario** is a brief description of an intended event or a series of events. A4Cloud has defined two types of scenarios:

- An "as-is scenario" is used to tell a story of current practice and focuses on the problem that needs to be solved.
- A "to-be scenario" describes how someone can accomplish something in the future. In this deliverable, to-be scenarios will be used to demonstrate how accountability mechanisms and tools can be used to solve the problems that have been outlined in the as-is scenarios.

The scenarios are written in natural language, in order to ease the process of producing subsequent iterations and receiving early feedback, both from stakeholders as well as from the different partners in the project.

A **UML use case** describes a system's behaviour under various conditions as the system responds to a request from one of the stakeholders. A UML use case describes how an actor initiates an interaction with the system in order to accomplish a goal. In this work package, UML use cases will be used as a technique for capturing functional requirements of the accountability mechanisms and tools that will be developed in the A4Cloud project.

⁸ Note that the project partners are not considered stakeholders in this context.

D:B-3.1 Use Case Descriptions

The main reason for developing scenarios and UML use cases is the major challenge associated with defining user needs of the accountability mechanisms and tools that the A4Cloud project will enable. One reason is that the stakeholders are often unaware of the many possibilities such technology will provide. Therefore it is important to both use an iterative approach for developing solutions, and to exploit scenarios and UML use cases for increasing our understanding of the user needs. Since a scenario is a story that describes a series of events and can be used to first describe the problem (the as-is scenario) and then to describe possible solutions (the to-be scenario), this approach makes it possible to start describing some of the most important needs for the relevant stakeholder, and use this as an input when choosing which business use case that will be instantiated in WP:D-7. The scenarios will also be important input to the dissemination activities in WP: A-3.

A4Cloud follows an iterative process. The scenarios will therefore be created in parallel with UML use cases, and they will all give input to each other. This document contains a first version of the scenarios, and the scenarios will be updated as the work with the business use cases progresses. The UML use cases are not part of this document, but will be presented in the next deliverable (D:B-3.2).

4 Business Use Cases

This section presents the three different business use cases (BUCs). As will be seen, the business use cases complement each other by dealing with different emerging issues in cloud ecosystems and they have different focus with regard to the central accountability questions that the project aim to address:

- BUC 1 ("Healthcare services in the cloud") is concerned with data aggregation in the cloud and involves a composition of two public IaaS clouds with a SaaS. It focuses on accountability for employing strong privacy by design mechanisms, and bringing out the link of accountability to support social requirements and privacy principles
- BUC 2 ("Cloud-based ERP software enabled with third party extensions") deals with hierarchical service layering in the cloud and involves a combination of a SaaS and a PaaS, running on top of a public IaaS. It focuses on dealing with the complexity of accountability relationships in complex supply chains (including about dynamisms in these leading to issues about how to build accountability while guarding against weak links in the chain)
- BUC 3 ("Rights and relevant obligations in a multi-tenant cloud") is concerned with multi-tenancy and the governance of personal and/or confidential data in the cloud. It involves different kinds of SaaS clouds, which may run on top of IaaS clouds. It focuses on accountability in multi-tenant environments. The issues raised by the two cases above are also relevant, but this one looks in particular at liabilities and responsibilities of the different actors and how appropriate obligations can be set and clarified to the parties involved.

The remainder of this section describes the different business use cases in details. Each subsection contains an overview of the BUC followed by an analysis of emerging accountability issues in the described cloud ecosystem. The description of each business use case also provides some usage scenarios and identifies the different actors that are involved in the cloud ecosystem.

4.1 BUC 1: Health Care Services in the Cloud

The first business use case concerns the flow of health care information from medical sensors to the cloud. The key motivation for including the health care domain in the A4Cloud project is the legal perspective related to the generation, processing, flow and traceability of sensitive personal information. This business use case demonstrates how the accountability mechanisms and tools that will be developed in A4Cloud can be used to protect sensitive health information as well as personal information. The specific example we will consider here concerns wirelessly networked sensors that are embedded in elderly people's living spaces or that can be carried on the person. Such sensors can be used to map their current health status, to analyse and diagnose their medical condition and analyse the effect of preventive measures. In the next subsections we will describe (a) why a cloud-based solution is desired when using medical sensor networks, (b) the issue of accountability in medical sensor networks, and (c) the use of such networks in the area of ambient assisted living (AAL).

4.1.1 Overview

In recent years there has been a significant growth in the use of wireless sensor networks in healthcare [13]. Sensor networks can be used for early detection of clinical deterioration through real-time patient monitoring in hospitals or at home, for improving the quality of life for the elderly through smart environments, and for monitoring of chronic diseases, to name just a few application areas. Common examples are sensors monitoring blood pressure, blood glucose, pulse oximetry, respiration rate, body temperature, physical activity and the patient's position (GPS). Realizing the potential of wireless sensors in healthcare requires addressing a multitude of technical challenges.

Healthy independent living is a major challenge for the ageing European population. The use of medical sensor networks offers unique proactive opportunities to, for example, support older people in their own houses. As people age, they experience a variety of cognitive, physical, and social changes that challenge their health, independence, and quality of life. Diseases such as diabetes, asthma, chronic obstructive pulmonary disease, congestive heart failure, and memory decline are challenging to monitor and treat. Wirelessly networked sensors embedded in people's living spaces or carried on the person can collect information about personal physical, physiological, and behavioural states and

D:B-3.1 Use Case Descriptions

patterns in real-time and everywhere. Such data can also be correlated with social and environmental context. The results can be used for self-awareness and individual analysis to assist in making behavioural changes, and to share with caregivers for early detection and intervention. At the same time such procedures are effective and economic ways of monitoring age-related illnesses.

While the number of patients is known or can be foreseen, the number of sensors and the amount of data that will be generated is more difficult to predict. Deploying the processing and storage of data from medical sensor networks in the cloud is a potential solution; not only because of cost advantages but also because of sensor networks' requirements for scalability and elasticity. A cloud infrastructure can handle the storage, processing, communication and visualization of the data, with streams of data arriving continuously from hundreds and thousands of sensors [14]. A cloud solution would also facilitate healthcare services to patients located in remote areas. Recently, medical sensors have incorporated wireless connections to communicate directly with cloud computing services [13].

4.1.2 Cloud Actors

The main actors involved in this business use case are

- The **business end users (cloud users)** are organizations that consume cloud services. In this business use cases the most significant business end users are the health care organizations that will be involved (in tis case the hospital and possibly also the primary care), the pharmacies that will provide the medication records, the research organizations and data analysis companies that will process anonymised medical data, and possible also insurance companies. In this business use case the hospital is ultimately responsible for the health care services and will hence act as one of the data controllers for the personal data that will be collected.
- The **individual end users (cloud users)**. In this business use cases there will be two different types of individual end users; the elderly persons from whom sensitive and personal data will be collected, and the elderly person's relatives and/or friends, who may upload personal data about the elderly. As will be seen in the subsequent analysis, the individual end users can act as data subjects or data controllers, depending on the context.
- One or more **cloud providers** that will operate cloud service resources on behalf of multiple cloud users. This business use case will involve cloud services for sensor data collection and processing, cloud services for data storage and cloud services for information sharing, which will be operated by a collaboration of different providers. It is expected that the primary service provider, with whom the cloud user will interface, will employ (at least) two sub-providers, thereby creating a chain of service delivery.
- One or more **regulators (cloud auditor)**. In the business use cases the Norwegian Data Protection Authority will be the main regulator involved.

This business use case will demonstrate how accountability mechanisms and tools can ensure the individual end users, the business end users, the cloud providers as well as the regulator that all actors involved in the storage and processing of personal data and sensitive personal data can be held accountable for the appropriate treatment of all the data that is passed into the cloud.

4.1.3 Emerging Issues in the Cloud Ecosystem

Wireless sensor networks in healthcare are used to determine the activities of daily living and provide data for longitudinal studies. It is then easy to see that such wireless sensor networks also pose a challenge to the patients' privacy. In this business use case we will investigate accountability aspects in medical sensor networks in the AAL domain. The system that we describe will be used to support the elderly by short-term and long-term analysis of behavioural and physiological data collected by wearable and environmental sensors. We will investigate a case where medical data from the sensors will be exchanged between the elderly, their families and friends, caregivers, health-care personnel, as well as a number of other actors who will be outlined below.

Using Figure 9 (Appendix B) we can analyse whether the involved actors are defined as data controllers or data processors according to Directive 95/46/EC [6]. In this business use case the

D:B-3.1 Use Case Descriptions

provider of Cloud z (who is also the primary service provider) will be seen as the controller with relation to personal data. It is the controller's responsibility to ensure that the data subjects' personal data is processed in line with the legal requirements, including the accountability obligations stated in the legislation. In this business use case the business end users will have contractual agreements with the primary service provider, which in turn will have contractual agreements with two other providers. This is illustrated in Figure 3 (the details in the figure will be further explained in the next subsection). Note that in this figure, the provider of Cloud x will be seen as a data processor, but since Cloud y is only used for storage and back up services as instructed by the primary service provider, the provider of Cloud y does not fall into the definitions of processor or controller⁹.

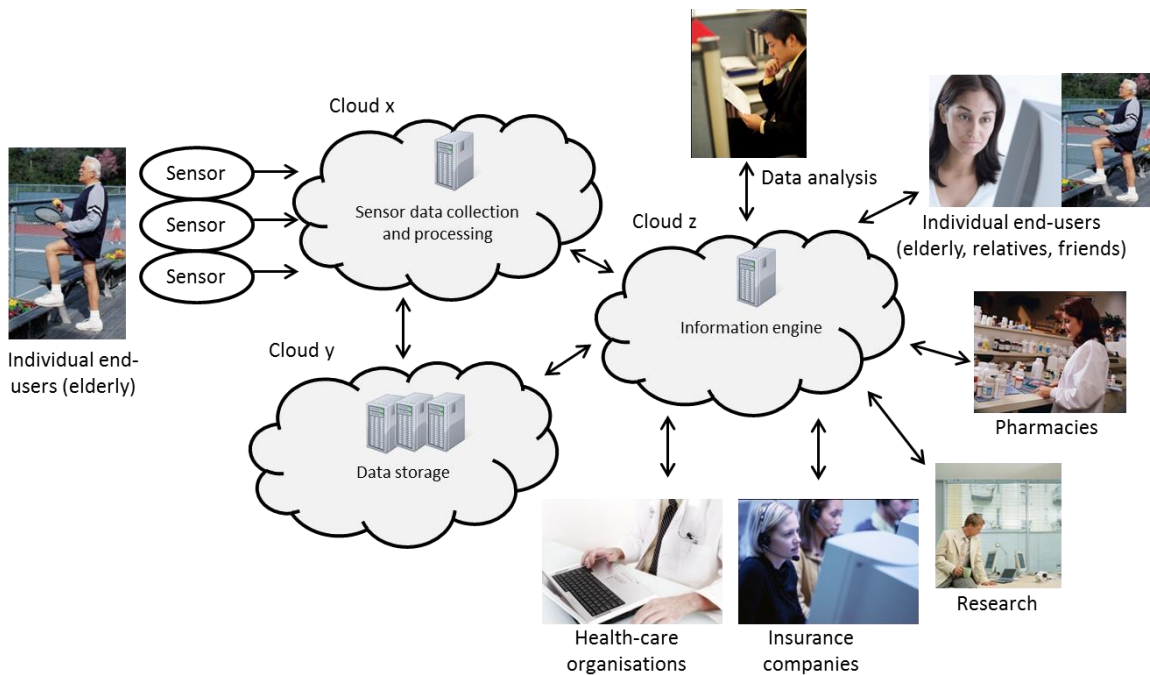


Figure 3 The MedNet platform

In this scenario where patients are cloud users, the patients will be defined as data subjects but the primary service provider is seen as the controller. However, other cloud users are identified in this scenario, such as friends/relatives of the patient. These other users can also be defined as controllers. Where friends/relatives have access to and can upload patient information (and set privacy policies in relation to how the data is used) they could be seen to determine means and purpose of processing¹⁰. Note that allowing relatives to have control over patient data should only be allowed in very special cases, since this give rise to many accountability challenges (see [12] for a discussion on who is accountable when users upload personal data about other users to a cloud).

In medical sensors network systems, there is a need to represent high-level aggregating requests such as querying the average, maximum, or minimum reading of specified sensor data. To retain privacy, this capability must be supported by anonymizing aggregation functions. This need arises for applications specially related to longitudinal studies. The use of such technology creates issues with respect to accountability obligations stemming from Directive 95/46/EC [6]. Medical data will be

⁹ As discussed in [15], when a cloud service comprises or includes permanent storage of data, the provider, it would seen that, the cloud service provider is likely to be a processor. However, for data stored in the cloud in encrypted form, or in fragments as non-personal data, in such a way that the personal data cannot be accessed by the provider, the provider should not be considered a processor.

¹⁰ Under the proposed regulation Article 24 would allow for actors to be defined as joint data controllers sharing responsibility and liability

D:B-3.1 Use Case Descriptions

"personal/sensitive data", but if it is properly anonymized¹¹ it is likely to fall outside the scope of the legislation and will not create any obligations on the controller and processor¹². This raises the question of accountability for the effectiveness of the anonymization, and who should be accountable if anonymization is inadequate.

In its opinion WP136 [17] the Article 29 Working Party has stated that the approach to anonymized data should be risk based. According to WP136, anonymized data may be considered non-personal data in the hands of another person (cloud provider), where the other person is specifically not intended to identify individuals, and appropriate measures have been taken to exclude re-identification by that person¹³. Further WP136 notes that, in such a situation, the information may not be "personal data" in the hands of the service provider if "the identification is not supposed or expected to take place under any circumstance, and appropriate technical measures (for example cryptographic hashing) have been put in place to prevent that from happening" - even if it is still theoretically possible to identify individuals in "unforeseeable circumstances", for example through "accidental matching of qualities of the data subject that reveal his/her identity" to a third party. The reason for this is that the information processed by the original controller (and now held by another person) may not be considered to relate to identified or identifiable individuals taking account of all the means likely reasonably to be used by the controller or by any other person [17].

Similar issues also arise with respect to aggregation of data which is often used to disguise identities, for example when releasing general statistics derived from research. Deleting or irreversibly changing direct identifiers such as names still leaves untouched the other information originally associated with the direct identifier. As an illustration, if information comprises name, age, gender, postcode and test results, and only the name is deleted or changed to a code number, information about each person's age, gender etc. still remains available. Indeed, usually the purpose of the deletion or change is to enable disclosure to others of the remaining information while attempting to disguise individual identities. That purpose would be defeated if age and, certainly in the example, test results had to be deleted before the information could be disclosed to intended recipients.

In this business use case, there is not only the processing of personal and sensitive data but also the storage of such data by a cloud provider (Cloud y in Figure 3). Data migrated to the cloud for storage will usually be encrypted. This involves encrypting the entire data set for security purposes, i.e. transforming or converting the entire original data set by applying a cryptographic algorithm to it. The issue is would such data constitute personal sensitive data under Directive 95/46/EC [6] and should accountability obligations be imposed on this provider.

In relation to the one who encrypts the data and holds the encryption (or, strictly, decryption) key, the information is likely to remain "personal data". However, if a cloud provider storing encrypted data on its servers has no access to the key and has no reasonable means to decrypt the data, under WP136 this information may be considered anonymous data. This might be the case, for example, where a SaaS provider uses a PaaS or IaaS provider's infrastructure to provide its own services (as in this business use case). Even if the SaaS provider has the key, so that it must treat the information as personal data, the PaaS or IaaS provider may not have the key.

If personal data has been strongly encrypted before being transmitted to the provider, provided the key was securely managed, the stored data would be unlikely to be considered "personal data" in the hands of the provider. Generally, "pure" cloud storage providers cannot control the form in which their users choose to upload the data to the cloud. In addition the provider would not necessarily know the nature of data the users intend to store. Yet the status of data stored with a cloud provider, which affects the status of the provider as "processor" (or not) of data stored by its users, will vary with each user's decisions and actions - which may differ for different users, and may even differ for the same user storing different kinds of data, or the same data at different times. Thus an important accountability (or perhaps more accurately transparency) issue is the communication of the status (for data protection purposes) of data between the uploading entity and the cloud provider.

¹¹ Note that the concept of "anonymised data" is not without controversy. There are generally accepted impossibility results of anonymising data while making the data useful, see for example [16].

¹² Data Protection Directive Recital 26

¹³ WP136 gives the example of "key coded data"

D:B-3.1 Use Case Descriptions

Sensor information traces captured by systems, such as the one in this scenario, are highly personal. Embedded in them is information that correlates with our identity and our behaviour. When combined with publicly available facts, these sensor information traces can be de-anonymized, and the data subjects' identities and life patterns can be revealed. Research has shown that, with developing techniques, information is increasingly linkable, and therefore individuals are increasingly identifiable [18]. It is possible, particularly with automated data mining methods operating quickly over huge quantities of information, to correlate, associate, combine or link and analyse different information, perhaps from different sources, all with reference to the same individual. Over time, increasingly more information can be gathered which is linkable to, and increasingly enables identification of, the same person [19].

Collecting data continuously as subjects go through their daily lives in their homes, in shopping centres, at leisure facilities and other places means that it is impossible to anticipate upfront, and accordingly inform subjects about, the complete nature of information that the sensor data may reveal. Some of the seemingly innocuous sensor data collected in relatively uncontrolled setting may capture information about confidential aspects of the data subjects' life patterns, personal habits, and medical conditions. One answer to these problems can be to allow the patients or their relatives to retain control over the raw sensor data throughout its life cycle, e.g., by putting restrictions on its capture, sharing, retention, and reuse.

In this business use case there is a need to represent different types of data owners and patients in the system as well as external users and their rights when different domains such as assisted living facilities, hospitals, GPs, and pharmacies interact. One of the more difficult accountability problems occurs when interacting systems have their own privacy policies. Consequently, inconsistencies in such policies may arise across different systems. For this reason, online policy consistency checking and notification along with resolution schemes are required. Note that the accountability mechanisms proposed in A4Cloud will not protect sensitive health information as well as personal information on their own – one will need privacy by design to be used in combination with anonymisation techniques, access control, purpose specification and data minimisation policies.

4.1.4 Usage scenarios

The A4Cloud eHealth business use case is being developed in cooperation with St. Olavs hospital in Trondheim, Norway. The business use case can be seen as a part of the coordination reform ("Samhandlingsreformen") that the Norwegian government initiated in January 2012¹⁴. The basic idea behind the coordination reform is to transform the Norwegian healthcare system into a more distributed organization. This is done through adopting preventive measures rather than just restorative actions and by moving health care services closer to the patients' premises. In A4Cloud we investigate a particular case of the coordination reform, which we have chosen to call "the Ageing Well program". The Ageing Well program includes the adoption of AAL technologies, which is used to improve the quality of life of elderly people and help them live safely in their homes. Amongst other things, the Ageing Well program will adopt methods that allow remote collection of long-term medical data needed in cases where symptoms come and go, that is, cases where making a diagnosis is considered particularly complicated. One concrete example is the diagnosis of balance disorders.

The current situation at St. Olavs hospital is that, after being subject to an examination by his GP, the patients have to stay in the hospital for a day during the diagnosis phase. Setting a diagnosis is challenging because the elderly usually suffer from several diseases, and there is a need to combine a lot of data from sensors, the patient record including current medication, and physical and mental tests. One challenge is that there is a need for long term monitoring in order to gather enough data to better understand the usually complex situation (sometimes up to 6-7 days), and to understand the effect of the medicine and training the elderly is doing. However, long term monitoring is too costly to do at the hospital. Another problem is that there is currently little support for automatic collection and processing of all the data that is needed to perform a diagnosis. Today, most of the data needs to be manually collected. The diagnosis also relies on data related to patient medication. However, the hospital does not have any possibility to access the medication journals that are stored at the GPs nor the lists of prescribed drugs that the patients have collected at pharmacies. Patients are therefore asked to bring

¹⁴ See <http://www.regjeringen.no/en/dep/hod.html?id=421>

D:B-3.1 Use Case Descriptions

all their medications to the hospital and, again, it is the nurses' tasks to record this information in the patient's hospital journal. After collecting all the necessary medical data, the data is anonymized and transferred to a server located in Australia where external actors are processing the data using a decision support system. The data is then transferred back to the hospital in Trondheim where it forms the basis for diagnosing the patient. All together, the current practice is considered to be extremely time consuming, expensive and not enabling the desired long term monitoring.

St Olavs hospital is now looking into more efficient processes, and is particularly interested in solutions where the long term monitoring of patients and the medical data collection can be done remotely, ideally from the patient's own home. The proposed solution that we will investigate further is the MedNet platform illustrated in Figure 3, which is a cloud-based platform for medical sensor data collection, processing, storage and visualization. Patients will be connected to wireless sensors that monitor their vital signs (e.g. movement, blood pressure, pulse oximetry temperature, position). The sensor data will be transmitted to the Cloud where it will be further processed and stored.

The MedNet platform will be developed by a Norwegian software and service provider, which will outsource both the sensor data collection and initial processing tasks as well as the long-term data storage and back-up procedures to one or more external cloud providers (Cloud x and Cloud y, respectively). The information engine, which visualizes and displays information to the end users, will be implemented in the Norwegian software and service provider's own private cloud (Cloud z). As can be seen in Figure 3, the MedNet platform will interact with and provide services to a number of different actors involved. The individual end users (the elderly and/or their relatives) will be able to access and review the data that has been stored about them, and will be able to retain control over their own personal information. Data analysis companies and research organisations will have access to anonymised medical data records. Physicians and caregivers at the hospital will have the full picture of the patient's medical condition; being able to monitor the readings in real time as well as to analyse data that has been processed by the data analysis companies, and access medication data from the pharmacies and patient's journal data that is locally stored at the hospital. This will give a complete and continuous view of the patient's health situation.

The medical data collected from the sensors may also be of interest to other actors, such as insurance companies. Compiling data from sensors monitoring blood pressure, heart rate, temperature, movement and medication will make it possible to estimate the risk of falls. Since a fall might result in a hip surgery, which is very costly and often requires a long period of institutionalization, this information may be of interest to insurance companies.

4.2 BUC 2: Cloud-based ERP Software Enabled with Third Party Extensions

The second business use case concerns cloud-based enterprise resource planning (ERP) software, extended by third party software as a service. Enterprise cloud deployments often involve several parties in the processing of personal data. The business use case describe here illustrates the case where ERP software, originally configured as an on premise system, can be extended with new capabilities combined with service extensions running on the cloud. Such extensions can involve different levels of outsourcing. In such a setting, accountability needs to be studied from multiple perspectives.

4.2.1 Overview

In this business use case we consider a cloud service (SaaS) for participants of a loyalty program offered by a supermarket chain called "MarchéAzur" (primary service provider and data controller). The service is accessible via a mobile shopping application that communicates with a back-end application deployed on a PaaS cloud offering by a company called "PaaSPort" (Subsequent Data Processor). "PaaSPort" utilizes infrastructure owned by IaaS provider known as "InfraRed". "InfraRed" provides virtualized infrastructure on which "PaaSPort" is running their PaaS cloud offering.

The supermarket's goal is to collect information about its customers' (data subjects') shopping behaviour that results in the creation of customer profiles (e.g., according to the age group, shopping behaviour, region he/she lives in). This profile could then be used to provide personalized shopping deals to customers. The supermarket's business partners may also want to access this information for marketing purposes (thus also becoming data controllers) – the customers who have given consent to this will receive direct advertisement from these partners. The back-end service for the supermarket

D:B-3.1 Use Case Descriptions

loyalty program uses a cloud persistency service (data processor) to store application data. The supermarket employees can make (depending on usage control rules) detailed database queries regarding the customers' shopping history and also create personalized offers via a web-based portal. Moreover, the cloud application exposes web services through which third parties interact with the back-end system to consume collected data.

The interface for the customers makes it possible to indicate privacy preferences with respect to the category of products (health care, food, drinks, etc.) that they want to share their shopping habits about (e.g. customer can opt-in for sharing his shopping history related to food but decline to do so for health care products). The information is used to produce personalized offers, so declining to share information about, e.g. health care products, need not result in the offers based on the products bought in this category. The customer can also indicate whether he permits the supermarket to share personally identifiable information with its business partners to send the personalized advertisement also from its partners. These choices should be reflected by the personal data access control mechanism, but there is no transparency for the supermarket's customers about how the controls work (e.g. customers have no way to check why they receive certain type of advertisement).

4.2.2 Cloud Actors

In our use-case scenario we are looking closer at the ERP system operated by a supermarket chain in the southern France ("MarchéAzur"). Apart from the on-premise ERP system MarchéAzur had also deployed an application in the Cloud that offers MarchéAzur customers (individual end users) the possibility to browse on-line product catalogues, put products on their wish-list (virtual shopping basket) and receive bargains (offers) regarding certain products. The application offers also business analytics functionality for the MarchéAzur employers (business end users) that among others consist mainly of customers' shopping history analysis per region, supermarket or product category. Figure 4 identifies these actors in the cloud landscape.

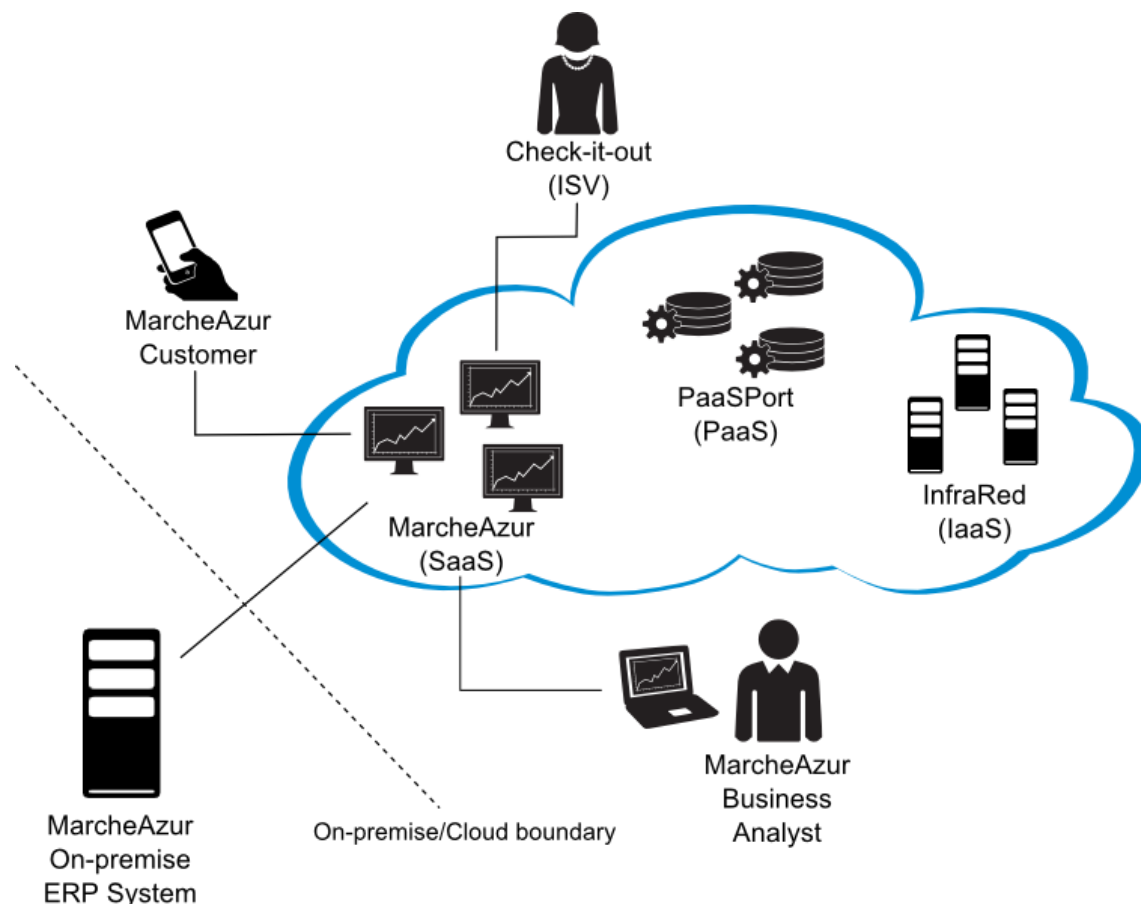


Figure 4 Actors involved in the ERP business use case

D:B-3.1 Use Case Descriptions

In this scenario MarchéAzur will be seen as a data controller under Directive 95/46/EC as it decides the means and purpose for processing personal data from the supermarket customers (individual end users). It will have an obligation to ensure that consent is obtained from the data subjects, that data is processed securely and fairly and that these obligations are enforced through the service delivery chain. To provide the analytics functionality, the cloud application makes use of High Performance Cloud Storage – a database which persists and processes all of this business data. The storage as well as transactional cloud offering managed by PaaSPort (data processor) is deployed on InfraRed IaaS infrastructure (processor). Besides, the MarchéAzur cloud application connects also to a third party software services managed by Independent Software Vendor, called “Check-it-out”. This actor could be defined as a processor but also a controller where it processes the data for its own purpose (see Figure 4), as Check-it-out provides a mobile payment solution for the products chosen by the customers.

MarchéAzur runs on-premise ERP system that stores business as well as personal data of their customers. Additionally it operates also application deployed on PaaSPort Cloud that exposes certain functionality to their customer (individual end users whose personal data is being stored and processed by cloud application). Apart from that, couple of other cloud services provided by Independent Software Vendors could be utilized by the MarchéAzur's cloud application to complete the initial functionality and provide additional functionality to the customers.

Meanwhile Independent Software Vendors (ISVs), like “Check-it-out”, that provides custom extensions to the cloud platform are also involved in personal data exchange. To complete this picture the operational activity of the cloud provider is also monitored by an external auditor (see Figure 4).

4.2.3 Emerging Issues in the Cloud Ecosystem

Within this business use case personal data is stored and transmitted between various entities. First, an on-premise ERP stores personal data about the customers: first name, last name, date of birth, address, etc. Inside the High Performance Cloud Storage system, much more information about the customers is stored (such as their shopping history, lists of presented offers, lists of accepted offers as well as information regarding the customers' lifestyle habits: eco-friendly, sports-person, family, etc) and cross-analysed against the data obtained from the on-premise system. To enable mobile payment for bought goods, the customers also need to send their credit card information to Check-it-out mobile payment service. As the data controller in this scenario MarchéAzur would need to ensure consent is obtained from all the supermarket customers (who are data subjects). A privacy policy presented to the customers informs them of what data is collected, how it will be processed and how it will be used. Under the proposed data protection regulation the controller should also state which processor/sub processors it will be relying on and ensure they impose appropriate security measures to meet the accountability obligations expressed in the legislation¹⁵.

As cloud applications can also access data initially stored in on-premise systems, the personal data changes not only logical location but potentially cross geographical boundaries where laws related to data handling could be different. Meanwhile, Independent Software Vendors (ISVs) that provide customised extensions to the cloud platform are also involved in personal data exchange. To complete this picture the operational activity of the cloud provider (PaaSPort) is also monitored by an external auditor.

Using cloud applications will result in in-house data being transferred to the primary service provider's data center but also to any third party providers relied upon by the primary provider. Under Directive 95/46/EC [6] there are strict restrictions on the transfer of data outside the European Union. Only countries, which have been approved by the commission as having adequate data protection standards can have data exported to them without further measures being taken. The issue with this restriction is that transfer of data to a server located outside the European Union is also accepted to be within the scope of article 25. Thus if a cloud user/controller uses a cloud provider based outside the EU or the service provider uses a subcontractor outside the EU, these would be seen as transfers within article 25. The focus in further work around this business use case is not merely on how the data is being processed but where and under which jurisdiction. As a controller MarchéAzur would

¹⁵ Proposed Regulation on Data Protection Article 26

D:B-3.1 Use Case Descriptions

need to ensure (usually through contractual agreements) that the cloud provider and any sub providers it relies upon keep the personal and/or confidential data within the EU.

An accountability framework would allow MarchéAzur to show evidence to corporate governance actors, auditors, but also customers that all obligations regarding personal data are being fulfilled across the full cloud supply chain of SaaS, PaaS and IaaS Cloud service models. This is the challenge for this business use case, and it can be expanded or restricted to focus on particular issues we might be interested of within A4Cloud.

4.2.4 Usage Scenarios

There can be multiple usage scenarios for this business use case. Its main focus is to facilitate the capitalization of customer data to retailing companies. As the cloud solution permits to easily deploy new applications to the platform as a service, the collection, analysis and sharing personal data with third parties is the major goal of the solution. Customer habits represent capital information for sales, and supplier relationships. The benefit for the customers would be customized offers and discounts, encouraging their fidelity, considering the ease of use and payment of the mobile software provided by the platform.

4.3 BUC 3: Rights and Relevant Obligations in a Multi-tenant Cloud

This section describes the third business use case, which is called "Rights and relevant obligations in a multi-tenant cloud scenario". The cloud ecosystem we consider consists of a number of players that must interact in a very agile manner in order to both preserve the value of the cloud paradigm and its benefits for end users and also to ensure that providers can appropriately and independently manage policies, controls and users of cloud resources. Such an ecosystem may be relatively simple with a one-to-one chain, but it may become extremely difficult to manage in its complex forms. Multi-tenancy – "the property of multiple systems, applications or data from different enterprises hosted on the same physical hardware" [10] – exposes organisations as well as individuals to merging issues in the cloud [1]. On the one hand, cloud computing is characterised by different characteristics (i.e. on-demand service self-service, broad network access, resource pooling, rapid elasticity and measured service) that enable complex operational data governance (exhibiting multi-tenancy, complex and dynamically changing environments, global and dynamic data flows, data duplication and proliferation, difficult to know geographic location and which specific servers or storage devices will be used, easy and enhanced data access from multiple locations). On the other hand, such cloud features expose organisations as well as individuals to cloud vulnerabilities [5] that emerge at the governance level. Data duplication and proliferation (and its autonomic aspect) creates problems in terms of compliance. In addition, public cloud providers make it very easy to open an account and begin using cloud services, and that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative, without due consideration of the risks and due governance process. There are also fears about increased access to data by foreign governments and other parties. Other issues include data lifecycle management across chains of suppliers, including data discovery and destruction, and legal risks that include security obligations, international transfers and the processing of sensitive data. For example, difficulties exist if users want to end a service, get their data deleted or export their data to another provider. Often, it is unclear who the data controller is and which parties have what responsibilities (MS-C2.2 provides further analysis of emerging issues in cloud service provision). In particular, key issues (as highlighted by the Article 29 Working Party [20]) are concerned with loss of control and transparency (in the sense of insufficient information, thus making the task more difficult of selecting a suitable service from the vast choice of cloud offerings).

4.3.1 Overview

The main features characterising this business use case are:

- **Personal and confidential data interaction:** individual cloud users increasingly access cloud services both for personal and business purposes. The blurred boundaries between personal and business confidential data are difficult to draw. Governing data flows becomes very complicated and exposes cloud users as well as cloud providers to emerging threats (e.g. data breaches and data loss) in cloud computing [1]. The problem is to clarify rights and obligations for cloud users and providers. Cloud users would benefit from awareness of how they comply with relevant

policies while accessing cloud services in business contexts. Cloud providers would be able to adjust their services according to individual as well as organisational policies.

- **Bring Your Own Device (BYOD):** individual end users increasingly access cloud services from within their business domains. This trend is exposing organisations to security threats – “*Security challenges due to social computing and bring your own device (BYOD) policies will increase as new vulnerabilities walk in the door with employees*” [2]. Identifying suitable policies for using personal devices to access cloud services is among the priorities for most organisations. The problem is to support the ability to verify whether or not specific data policies are satisfied while accessing cloud services.
- **Multi-tenancy:** the scenario focuses on data governance conflicts arising in the interaction between personal and confidential data flows. Conflicting and competing requirements are to a certain extent due to the nature of multi-tenancy – “*Multi-tenancy in its simplest form implies use of same resources or application by multiple users that may belong to same organization or different organization*” [13]. The problem is to guarantee policies throughout chains of accountability while services are accessed by multiple cloud users.
- **Data governance:** moving to the cloud introduces a separation between data subjects and the location where data is stored in the cloud. This ‘*distance*’ between data subjects and their data increases the complexity of data governance as well as the risk of loss of governance. This is due to delegating responsibilities throughout cloud supply chains. Supporting data governance for cloud users and providers enhances cloud trustworthiness.

4.3.2 Cloud Actors

This section identifies the main cloud actors that are relevant for the cloud ecosystem we are concerned with. From a business perspective, various stakeholders may be relevant depending on specific operational and deployment situations. Figure 5 shows the cloud ecosystem.

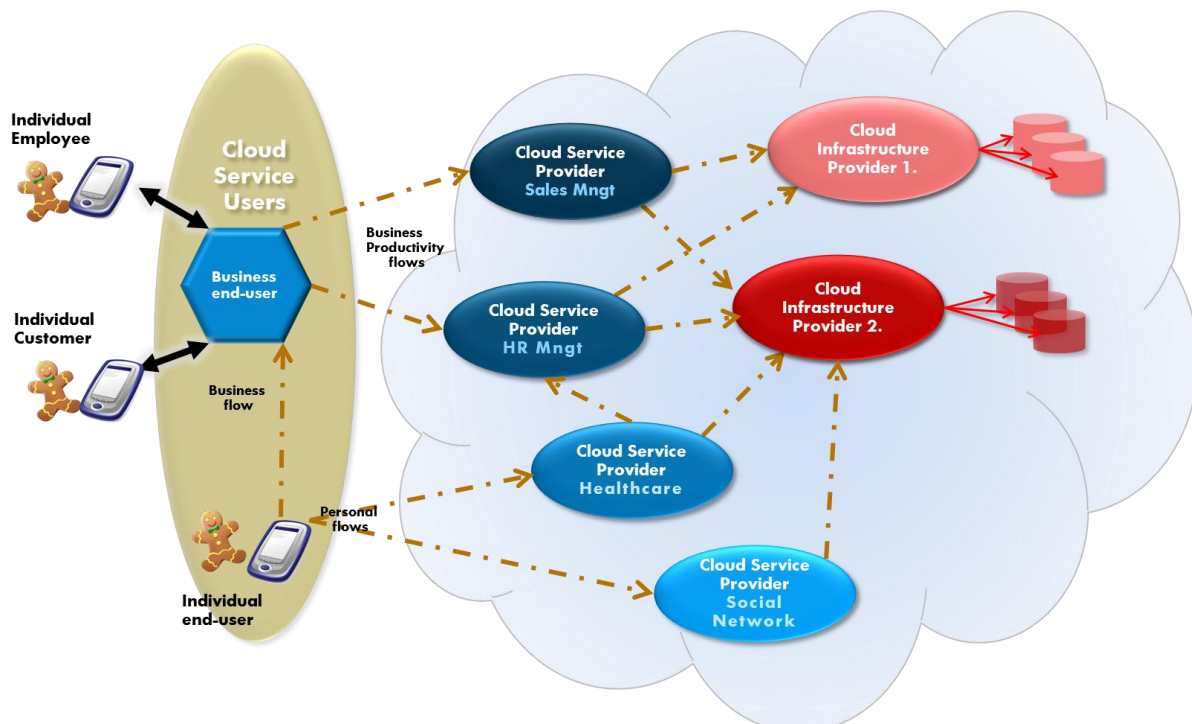


Figure 5 Cloud ecosystem for the multi-tenancy business use case

The actors involved in this business use case’s cloud ecosystem cover the following roles (classified according to the A4Cloud project’s taxonomy of stakeholders):

D:B-3.1 Use Case Descriptions

- **Cloud infrastructure provider (cloud provider):** a cloud infrastructure provider (IaaS provider) will manage and operate infrastructure resources on behalf of multiple cloud providers, and hence need to be able to enforce controls required by the end user.
- **Cloud service provider (cloud provider):** a cloud service provider (SaaS provider) will typically operate service level resources on behalf of multiple cloud service users, and sometimes on behalf of other cloud service providers (service aggregation). Hence they need to be able to enforce controls as agreed with their users. For example, a cloud service provider may be a SaaS provider, operating on an IaaS provider infrastructure, and delivering the SaaS service to many enterprises, businesses, or individual end users.
- **Cloud service user (cloud user):** a cloud service user could be an individual, or a business. When it is a business it adds another actor down the chain, typically a customer or employee of the cloud service user. In addition, aggregation of cloud services at each layer (e.g. IaaS, SaaS) means that the chain of actors can extend horizontally across providers before they reach a service user or an individual end user.
 - **Individual end user (cloud user):** an individual end user is usually the entry point to the chain and the provider (data subject) of the personal data which may be at risk along the processing chain.
 - **Business end user (cloud user):** a business end user may deserve a specified level of protection in terms of rights and obligations in order to preserve business confidential data. These rights and obligations may differ from applicable regulatory requirements due to data protection law. Moreover, some business domains (e.g. healthcare) may have additional regulatory obligations of confidence which need protecting.

4.3.3 Emerging Issues in the Cloud Ecosystem

The cloud ecosystem, in this business use case, may become extremely dense, interwoven and dynamic. Therefore, it is critical that the different actors are able to have a common understanding of where accountability lies in the control, configuration, and operation of the different services. As with many cloud scenarios the issue of control over the processing of personal and confidential data is crucial to determine and allocate responsibility. Complexities arise in the context of multi tenancy scenarios. In this situation, the SaaS provider could be a controller with respect to data it collects and could even be considered a processor in connection to the personal data of the user, which it uses for its own means (see Figure 9 on controller/processor under Directive 95/46/EC. Thus direct accountability obligations stemming from the legislation should be applied to the actor (the same rationale could also be applied to social network sites). When the service provider is relying on an infrastructure provider, it is hard to define such actors as controllers or processors within the scope of the legislation. Although they manage and operate resources that the cloud service provider will use to process end user data they do not have access to this data especially in the above scenario where confidential data might be encrypted before migration.

Individual end users are increasingly going to be using a single device for personal and business use, accessing cloud-services for personal and business purposes from the same device (Bring Your Own Device – BYOD). In this particular scenario, the individual end user (cloud user) accesses cloud services for storing personal data (in this case, acting as data subject) and works for a business end user (cloud user) that relies on cloud services (in this case, acting as cloud controller) for storing confidential data. In general, any individual end user might act as data controller or processor as well as being a data subject depending on individual responsibilities derived from the specific cloud ecosystem. As a result, end user client devices will be at the intersection of policy enforcement of different IT domains with which users interact via cloud services, thus raising new accountability challenges. To the extent that a user's personal data may be replicated or synchronised with cloud data storage services, data governance issues span across devices and cloud services. Similarly, data governance issues will apply to enterprise data as it is cached or replicated across a potential range of end user devices that may be increasingly end user owned devices. However, data controller responsibilities do not end or reduce because they do not own the device that has access to the data. The same degree of control and protection is still expected notwithstanding that it might be more difficult. Introducing new vulnerabilities will not be excused. The regulator's expectation is that the threats should be identified and resolved. With BYOD in the cloud environment the obligations, which

D:B-3.1 Use Case Descriptions

a controller should be aware of, include consideration of a device being used to access a cloud service, which permits users to remain logged in between sessions, unauthorized access to the device could easily result in an unauthorized disclosure of personal data as well as confidential data. In addition to this, devices may offer additional protection through the option to sandbox or ring-fence data, for example by keeping data contained within a specific app. If this is the case, and the controller is relying on this as a security measure, consideration should be given on how to verify these features in order to ensure the confidentiality and integrity of the data. Devices may also offer the ability to restrict access to certain apps or data types based on geographic location or require an additional level of authentication. Some devices may offer an automated backup facility, which stores a backup of data on the device to the user's cloud-based account or to the user's personal computer. A data controller will need to ensure that, if this facility is enabled, it will not lead to an inappropriate disclosure of personal data as well as confidential data.

4.3.4 Usage Scenarios

We will analyse a case that reflects a simplified version of the described ecosystem, where end users operate personal devices to interact with two different IT domains via cloud services:

1. An employer enterprise ecosystem and its business productivity cloud applications
2. A healthcare IT domain via e-government type cloud services available to citizens.

End users will also operate with personal applications on the same device, identifying a personal IT domain. From a cloud service perspective, we will assume a single IaaS provider that operates both the enterprise employee cloud application services and the government health care cloud service, in order that we can analyse accountability modelling and tracking at the intersection of the end user, IaaS provider, enterprise, and healthcare service operator. We will further assume that at least one of the cloud service providers relies on a cloud service provided by yet another cloud service provider. Finally, we will analyse how to ensure accountability of the enforcement of confidentiality and integrity guarantees over employee personal data, personal healthcare data and enterprise business data across the stakeholder interfaces.

5 Scenarios

This section explains how we have utilized scenarios for describing the use of accountability mechanisms and tools in the three different business use case domains.

5.1 The Role of Scenarios in A4Cloud

A scenario is a hypothetical story, which can be used to help a person think through a complex problem or system. The motivation for using scenarios in A4Cloud is:

- To describe different user situations as a fundament for developing UML use cases and requirements
- To be used as a tool for creating shared mental models of the project's goals among the different partners involved.
- To help communicate specific usage scenarios to relevant stakeholders and help them reflect how the A4Cloud tools and technologies can be of value.

The scenarios will be used to illustrate how the accountability mechanisms and tools that will be developed in A4Cloud can solve some of the accountability concerns that have been identified.

In A4Cloud we will use as-is scenarios (that tell a story of current practice) and to-be scenarios (that tell a story about someone trying to accomplish something with the A4Cloud accountability mechanisms and tools in the future).

5.2 Developing Scenarios

The scenario development is essential to get a good start in the project. Since the requirements derived from the scenarios will guide the development of accountability mechanisms and tools in the rest of the project, it is important that all partners use their knowledge and expertise as input to this process. By providing relevant scenario descriptions all partners will have influence in setting the path for A4Cloud. The scenarios developed in in this deliverable have therefore been subject to several rounds of internal review by other project partners who are not directly involved in this work package.

As illustrated in Figure 6, functional requirements (UML use cases) will be derived from the to-be scenarios. These will be then delivered WP:D-7 and used in the preparation of the demonstration and evaluation of the accountability mechanisms and tools that will be developed in A4Cloud. In addition, as explained in Section 1.1, several other work packages in A4Cloud will use the scenarios as input to their development work.

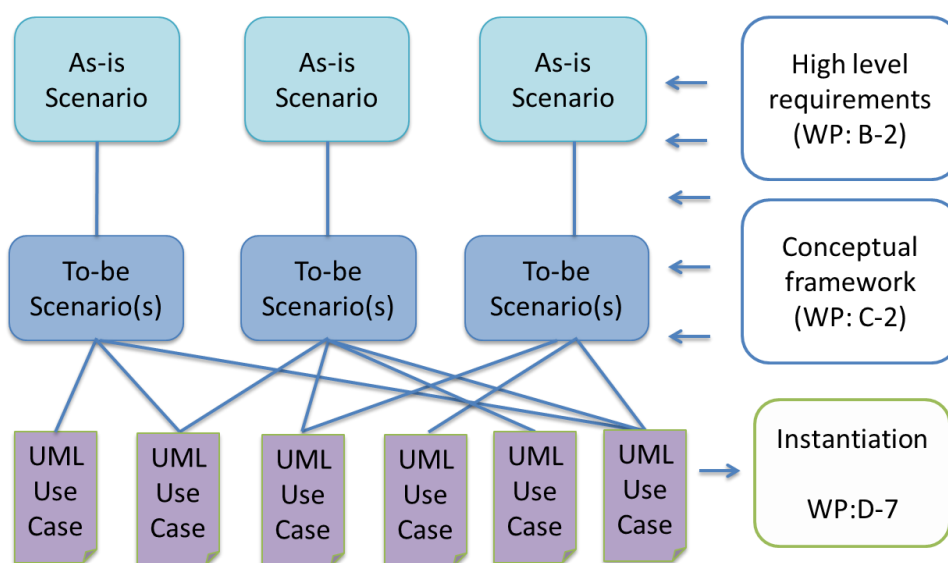


Figure 6 The relation between as-is scenarios, to-be scenarios and UML use cases

An **as-is scenario** tells a story of current practice. These stories are carefully developed to reveal problematic aspects of current practices in the problem domain. The as-is scenario will tell the reader

D:B-3.1 Use Case Descriptions

why the people involved are doing what they are doing and what they want to achieve. When identifying as-is scenario we have identified possible users, defined their problems, analysed their interests and objectives. This information has been extracted from interviews with users and other stakeholders, locally organized workshops, and related work. The as-is scenario and their stories have implications for design of the to-be scenarios.

To-be scenarios are stories about someone trying to accomplish something with a product or system in the future. To-be scenario involves writing a story that involves new ways of thinking about the users' needs and how they can be met.

A story in a to-be scenario may involve several technologies that will be developed in A4Cloud. The strength of the scenario is that it helps discover problems in the relationships between the A4Cloud tools. A very important characteristic of a to-be scenario is ease of evaluation—that is, when testing a scenario it should be easy to tell whether the accountability mechanisms and tools developed in A4Cloud are able to address the expressed accountability concerns.

To describe different actors/roles in a scenario we use a number of **personas**. Developing and using personas is a common method for defining and getting to know the target users of a computer system. The personas are not real users but fictional portraits of users. Attributes that are common to include when describing a persona are his/her name and age, a picture, motivation/goals, computer skills, a short personal history, employment and job description. When writing the scenarios we have identified a number of **accountability concerns** that these users experience and described how accountability mechanisms and tools will handle them. Through the workshops and interviews with important stakeholders in the different business use case domains (these efforts have been driven by WP:B-2), we have identified a number of important end users who will interact with the tools that will be developed in A4Cloud, and we have outlined a set of personas to generalize and illustrate their concerns.

5.3 Guidelines for Creating a Scenario

We have relied on the following guidelines when outlining the scenarios:

- The scenario must be important for the A4Cloud stakeholders
- The scenario must illustrate at least one important accountability concern, for at least one of the cloud actors identified in Section 2.
- The scenario must be suitable for demonstrating the effectiveness of accountability mechanisms and tools

The scenarios for business use case 1, 2 and 3 are presented in Appendix C, D and E, respectively.

6 Accountability Relationships in the Business Use Cases

In this section we analyse the to-be scenarios from the three different business use cases, in terms of what accountability attributes they comprises.

The A4Cloud Conceptual Framework (WP:C-2) has identified a set of accountability attributes, which are concepts that are considered part of, or that support, accountability. The three most prominent of these attributes are *responsibility*, *liability* and *transparency*. A brief description of these three attributes (taken from [11]) is:

- **Responsibility** can be defined as the state of being assigned to take action to ensure conformity to a particular set of policies or rules. A responsible entity is one that is assigned to take action to ensure conformity to a particular set of policies and rules. Responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to centre 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
- **Liability** is the state of being liable (legally responsible). A liable entity is an entity which is legally responsible for the (legal) consequences of a certain action. Liability can be explained as an obligation (either financially or other penalty) in connection with failure to apply governing rules and/or honouring commitments; liability is an element of almost every definition of accountability
- **Transparency** involves operating in such a way as to maximise the amount of and ease-of-access to information which may be obtained about the structure and behaviour of a system or process. It is an attribute of an object, process or system that its creation or behaviour can be observed. Transparency describes the property of an accountable system or service that it is capable of "giving account" of, or providing visibility of how it conforms to its governing rules and commitments.

Several other accountability attributes have been identified in the conceptual framework working document [11]. To give the overall picture we briefly describe the remaining attributes. **Observability** is concerned with the cloud "behaviour". It describes how well the internal actions of a cloud service can be described, by just looking at the input/output of the service. **Verifiability** is concerned with the ability to verify the behaviour of a service against a set of given requirements. **Attributability** is concerned with identifying causes of behaviour (Who did what? Was it a service glitch or a deliberate action?).

Figure 7 describes the cloud-mediated interaction between two generic actors (Actor A and Actor B) in terms of all these accountability attributes. It shows the scope (according to our understanding) of the accountability attributes. As can be seen, transparency relies on verifiability and attributability, which in turn rely on observability. Similarly, responsibility and liability rely on transparency. As shown in the figure, accountability encompasses all the accountability attributes.

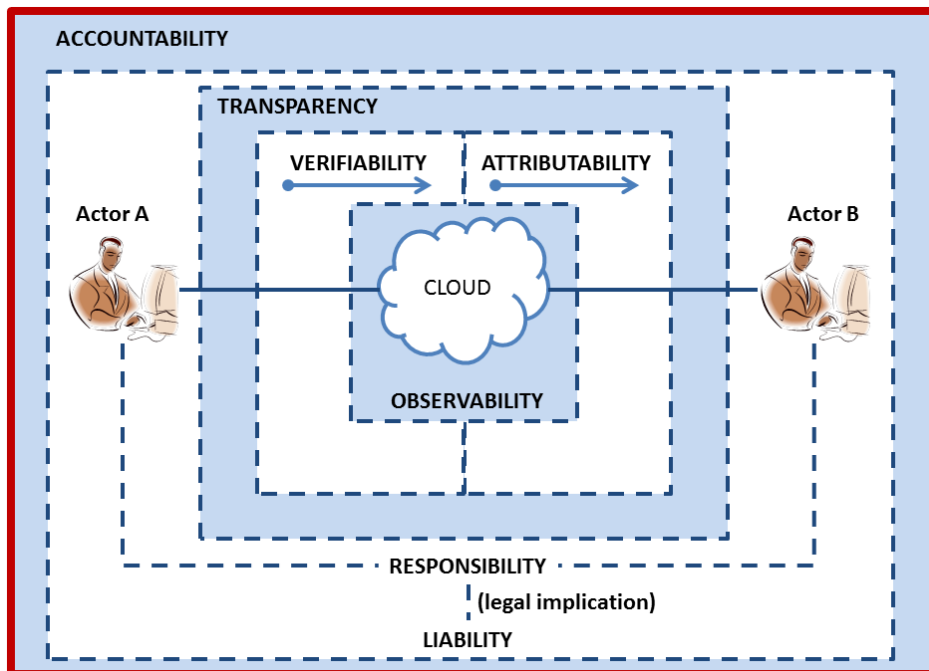


Figure 7 The role of the accountability attributes in the interactions between actors

Other aspects of accountability have been also discussed in the conceptual framework working document. **Sanctions** are the (legal) consequences of failing to comply with some requirement. **Assurance** is a positive declaration intending to give confidence. Assurance can take the form of evidence, which can be used to convince a third party about, for example, the reason for a failure that has happened. Finally, **remediation** is the act or process of correcting, for example a failure or deficiency. Note that the A4Cloud conceptual framework is currently being revised, which means that the set of accountability attributes and their interpretations may be subject to changes [11].

In the remaining parts of this section we analyse each business use case (as they have been described in the previous three sections and the appendices) in terms of what accountability relationships that exist in the scenarios. For each to-be scenario we have identified the actors involved and the personal and/or confidential data exchanged between them, and then identified the accountability attributes that apply. We use matrices to highlight the accountability relationships in terms of attributes amongst the actors. As a starting point we have focused on the three top-level attributes responsibility, liability and transparency (but note that the other attributes will be relevant, since transparency depends on them in order to give specific visibilities of data governance and accountability in the cloud). Hence, it is possible to define chains of accountability by taking into account the relationships described in the matrices.

Section 6.1 - 6.3 describe the accountability relationships that we have identified for the three different BUCs. Each accountability relationship is traced from the scenario that it originates from. Note that in some cases we have identified additional relationships, which do not have any reference to any scenario. The results are formulated to a tabular format, in which an association of the actors to taxonomy of the cloud actors is provided, along with the relationships between the roles with respect to the accountability core elements.

6.1 Accountability relationships in Business Use Case 1

The roles [actors] involved in this business use case are:

- Patient [cloud user]: the individual end user who shares personal data (name, age, location) and sensitive information (blood pressure, oxygen saturation, health record)
- Relative/friend [cloud user]: the individual end user who uploads further information about the patient
- Hospital [cloud user]: the organization that diagnosis the patient and decide the appropriate treatment.

D:B-3.1 Use Case Descriptions

- Cloud provider x [cloud provider]: the organization that operates the sensor data collection and processing cloud (Cloud x)
- Cloud provider y [cloud provider]: the organization that operates the data storage cloud (Cloud y)
- The MedNet platform provider [cloud user, cloud provider]: the organization that delivers the software for sensor data collection and processing to the hospital and that operates Cloud z.
- The Norwegian Data Protection Authority [cloud auditor]: the organisation that verifies that statutes and regulations that apply to the processing of personal data are complied with, and that errors or deficiencies are rectified.

Table 1 The accountability relationships between the actors involved in BUC1

ID	Accountability relationship	Accountability Attribute	Scenario
R1	The relative/friend is responsible to the patient for adhering to the patient's privacy preferences when uploading personal data about the patient	Responsibility	Scenario 2.1.1a
R2	The hospital is responsible to the patient for asking the explicit consent for collecting and processing personal data	Responsibility	Scenario 1.1.1a Scenario 1.1.2a
R3	The hospital is responsible to the patient for asking the explicit consent for allowing relatives to access personal data	Responsibility	Scenario 2.1.1a
R4	The hospital is responsible to the patient for using personal data for the specified purpose only	Responsibility; Transparency	Scenario 1.1.1b Scenario 1.1.1c Scenario 3.1.1a Scenario 3.1.1e
R5	The hospital is responsible to the patient for informing them about data handling practices.	Responsibility; Transparency	Scenario 1.1.1a Scenario 1.1.1b Scenario 1.1.1c
R6	The hospital is liable to the patient in case of personal data loss or misuse	Liability	N/A
R7	The hospital is responsible to the Norwegian Data Protection Authority for using personal data in accordance to applicable rules and legislations	Responsibility	N/A
R8	The hospital is responsible to the Norwegian Data Protection Authority for proving evidence on the data collection practices	Responsibility; Transparency	Scenario 1.1.1c
R9	The hospital is responsible to the Norwegian Data Protection Authority for informing about the collection and processing of personal data	Responsibility; Transparency	N/A
R10	The MedNet platform provider is responsible to the hospital for logging all access to personal data	Responsibility; Transparency	Scenario 1.1.1b
R11	The MedNet platform provider is responsible to the hospital for informing about 3 rd party service providers in the service deliverable chain	Responsibility; Transparency	Scenario 3.1.2a
R12	The MedNet platform provider is liable to the hospital when including 3 rd party service providers in the service deliverable chain	Responsibility; Liability	Scenario 3.1.2a
R13	The MedNet platform provider is responsible to the hospital for fulfilling their contract terms	Responsibility	Scenario 3.1.1a Scenario 3.1.1c Scenario 4.1.1b
R14	The MedNet platform provider is responsible to the hospital for proving evidence on the data processing practices	Responsibility; Transparency	Scenario 3.1.1b Scenario 3.1.1d
R15	The MedNet platform provider is responsible to the hospital for notification of security or privacy breaches	Responsibility; Transparency	Scenario 3.1.3a
R16	The MedNet platform provider is liable to the hospital in case of personal data loss or misuse	Liability	N/A

D:B-3.1 Use Case Descriptions

R17	Cloud provider x is responsible to the MedNet platform provider for the security of the provided service	Responsibility	N/A
R18	Cloud provider x is responsible to the MedNet platform provider for proving evidence on the data processing practices	Responsibility; Transparency	Scenario 4.1.3a
R19	Cloud provider x is responsible to the MedNet platform provider for fulfilling their contract terms	Responsibility;	N/A
R20	Cloud provider x is liable to the MedNet platform provider in case of personal data loss or misuse	Liability;	N/A
R21	Cloud provider y is responsible to the MedNet platform provider for secure storage and back-up of sensor data	Responsibility; Transparency	Scenario 5.1.1a
R22	Cloud provider y is responsible to the MedNet platform provider for correct and timely deletion of stored sensor data	Responsibility; Transparency	Scenario 1.1.2c Scenario 1.1.3a
R23	Cloud provider y is responsible to the MedNet platform provider for the security of the provided service	Responsibility;	N/A
R24	Cloud provider y is responsible to the MedNet platform provider for proving evidence on the data storage practices	Responsibility; Transparency	Scenario 4.1.3a Scenario 5.1.1a
R25	Cloud provider y is responsible to the MedNet platform provider for fulfilling their contract terms	Responsibility;	
R26	Cloud provider y is responsible to the MedNet platform provider for notification of security or privacy breaches	Responsibility; Transparency	Scenario 4.1.3a
R27	Cloud provider y is liable to the MedNet platform provider in case of personal data loss or misuse	Liability;	N/A
R28	The Norwegian Data Protection Authority is responsible to the patient for monitoring that the rules and legislation for protecting personal data are being obeyed	Responsibility;	Scenario 6.1.1a
R29	The Norwegian Data Protection Authority is responsible to the patient for controlling that incorrect usage of personal data is corrected	Responsibility;	Scenario 6.1.1b

6.2 Accountability relationships in Business Use Case 2

The roles [actors] involved in this business use case are:

- The supermarket customer [cloud user]: the actor that shares personal (i.e. name, age, location, shopping behaviour, etc.) and financial information (i.e. credit card number)
- The supermarket chain [cloud user, cloud provider]: the actor that processes the customers' data and notify them of the offers, defines the policy for making use of the customers' data and behaviour in order to formulate offers
- Third-party service provider [cloud user, cloud provider]: the actor that retrieves the super market customers' information to send additional advertisements
- PaaS owner [cloud provider]: the actor deploying the platform through which data is collected and distributed among the end users
- IaaS provider [cloud provider]: the actor that provides the public infrastructure for storing data and facilitating the communication
- Regulator [cloud auditor]: the actor providing the legal framework that governs the information exchange among the users and providers.

Table 2 The accountability relationships between the actors involved in BUC2

ID	Accountability relationship	Accountability Attribute	Scenario
R1	The supermarket customer is responsible to the supermarket chain for providing correct identification information	Responsibility	N/A
R2	The supermarket chain is responsible to the supermarket customer for processing data according to the customer preferences	Responsibility	Scenario 7.1.1a
R3	The supermarket chain is responsible to the supermarket customer for providing the evidence that the data was processed accordingly	Responsibility; Transparency	Scenario 7.1.1b Scenario 7.1.1c
R4	The supermarket chain is responsible to the supermarket customer to send only the offers that are related to the customer's preferences	Responsibility	Scenario 7.1.1a
R5	The supermarket chain is responsible to the supermarket customer to share with the third-party service provider only the information required for the business needs of the latter	Responsibility	N/A
R6	The third-party service provider is liable to the supermarket chain in case of the lose control over the supermarket customer data	Liability	N/A
R7	The third-party service provider is responsible to the supermarket chain to inform it about any changes related to the handling of the data received for providing the business purpose	Responsibility	Scenario 8.1.1b
R8	PaaS Owner assures the supermarket chain and the third-party service provider that the correct measures protecting from unauthorized data access are in place	Assurance	Scenario 9.1.1a
R10	The supermarket chain should be held responsible in case of the lose control over the supermarket customer data	Liability	N/A
R11	The third-party service provider should give a clear explanation why the data he collects from the supermarket chain is necessary for providing the service	Transparency	N/A
R12	IaaS Owner is liable to the PaaS Owner over any security breach in the infrastructure	Responsibility; Liability	N/A
R13	The regulator is responsible to assure the supermarket customer that the supermarket chain processes the data accordingly	Responsibility	N/A
R14	The supermarket chain is responsible to provide the necessary data to the regulator during the audit	Responsibility; Transparency	Scenario 12.1.1a
R15	PaaS Owner should notify the supermarket chain and the third-party service provider in case of any security incident related to the platform	Responsibility; Transparency	N/A

6.3 Accountability relationships in Business Use Case 3:

The roles [actors] involved in the cloud ecosystem of BUC3 are:

- The individual end user [cloud user] : the actor that provides their personal data in the cloud
- The business end user [cloud user]: the actor that provides their corporate data in the cloud
- The cloud service user [cloud user]: the actor that consumes the results of a service chain
- The cloud service provider [cloud provider]: the actor that offers services over the cloud
- The cloud infrastructure provider [cloud provider]: the actor that is responsible to secure the appropriate infrastructure resources, so that the cloud services can be executed.

Table 3 The accountability relationships between the actors involved in BUC3

ID	Accountability relationship	Accountability element	Scenario
R1	The individual end user is responsible for selecting the personal data to be placed in the cloud	Responsibility	Scenario 13.1.1
R2	The business end user is responsible for providing the corporate data to be placed in the cloud	Responsibility	Scenario 14.1.1.
R3	The cloud service user is responsible for accepting the results provided by the cloud service providers	Responsibility	Scenario 14.1.1; Scenario 15.1.1
R4	The cloud service provider is responsible for maintaining the integrity of the cloud-based personal data delivered to the cloud service users	Responsibility	Scenario 15.1.1
R5	The cloud infrastructure provider is responsible for preventing any unauthorised access to the resources of the cloud ecosystem	Responsibility	
R6	The cloud service provider should pay penalty when data used for the service to be offered are leaked to other service providers without the cloud (individual or business) end user consent	Liability	Scenario 16.1.1
R7	The cloud infrastructure provider should pay penalty to cloud service provider and/or cloud service user on data misuse	Liability	Scenario 16.1.1
R8	The cloud service provider should make an analysis of risks from the misuse of cloud end users' data in the cloud	Transparency	Scenario 15.1.1
R9	The cloud service provider should make explicit which cloud end users' personal and sensitive data are necessary to offer the service on the cloud	Transparency	Scenario 15.1.1
R10	The actions performed by the cloud service provider and the cloud service user when accessing personal and sensitive data should be logged	Transparency	Scenario 15.1.1
R11	The cloud service provider assures that the process of data stored in the cloud is compliant with regulatory frameworks and the business policies of the service provider	Responsibility; Liability	Scenario 15.1.1
R12	The cloud infrastructure provider assures that no data is leaked outside the scope of the underlying applications	Responsibility; Transparency	

7 High-level Functional Analysis of the To-be Scenarios

In Appendix C-E we outline a number of to-be scenarios, which described how stakeholders can use accountability mechanisms and tools to solve a set of accountability concerns. These to-be scenarios are highlighting some of the accountability enabling mechanisms that will be developed in this project. In this section we provide a high-level functional view of the to-be scenarios, which has been organized in terms of cloud actors. The references to the scenarios make it possible to track in which scenarios the use of a particular functionality has been described. The functionalities derived from the high level functional view of the to-be scenarios are tabulated in the next subsections, with one table for each cloud actor. The functionalities are split into four main categories of functionality, namely *policy management*, *data governance*, *risk analysis* and *compliance and auditing*.

7.1 Functionalities for individual end users (cloud users)

This section summarises the functionalities, which have been identified for the individual end users in the scenarios reflecting the domains of the three business use cases. In principle, this kind of cloud actor can impact the processes on policy management, data governance and compliance checks. The functionalities are allocated to these three categories, as shown below.

Table 4 Functionalities for individual end users (cloud users)

ID	Functionality	Description	Source scenario(s)
<i>Policy Management</i>			
F1-1	Edit policy	Create, modify or delete a user policy about the use of personal data	1.1.2a (Kim), 2.1.1b (Sandra), 13.1.1a (Sandra)
F1-2	Edit access rights	Set, view and modify access rights to personal data	1.1.2b (Kim), 7.1.1a (Alice)
F1-3	Configure time period of use	Set the time period for keeping personal data in the cloud	7.1.1c (Alice)
F1-4	Delegate right to reconfigure policy	Allow another cloud actor change the configuration of a specific user policy	2.1.1b (Sandra)
F1-5	Accept policy	Accept the policy of a cloud provider/cloud service user	Derived from F1-4
F1-6	Accept purpose of use	Accept the purpose of use of personal data from specific cloud provider/cloud service user	Derived from F1-4
F1-7	Select policy	Browse sample policies and select policy for the use of personal or confidential data	13.1.1b (Sandra)
F1-8	Receive policy notification	Receive notifications on the status of the policy enforcement of the cloud provider/cloud service user, including policy violations	8.1.1b (Bob), 13.1.1e (Sandra), 13.1.1g (Sandra)
F1-9	Report violation	Report any policy violation experienced in the use of cloud services	13.1.1f (Sandra), 18.1.1b (Sandra)
F1-10	Report infringement	Report a misuse experienced in cloud provider/cloud service user implementing accountability practices	18.1.1b (Sandra)
<i>Data Governance</i>			
F1-11	View policy settings	Request to explore the fields comprising the user policy on governing the use of personal data	1.1.1a (Kim), 7.1.1b (Alice)

D:B-3.1 Use Case Descriptions

ID	Functionality	Description	Source scenario(s)
F1-12	Select data	Decide which personal data can be transferred outside the primary service provider's own IT systems	1.1.2c (Kim), 1.1.3a (Kim), 2.1.1a(Sandra), 7.1.1a (Alice)
F1-13	Edit data	Correct or delete the personal data used (even if they are "in the cloud")	Derived from F1-12
F1-14	Track data	Track the use of personal data (including data "in the cloud")	1.1.1b (Kim)
F1-15	Analyse use	Analyse the trace on the use of personal data with respect to how data is stored by the cloud provider, what data have been collected, for what purposes and when and who accessed this data	Derived from F1-14
F1-16	Request data tracking	Select which personal data used "in the cloud" should be tracked	Derived from F1-14
F1-17	Receive notification on data management	Receive notifications on actions with respect to data management, based on user policy (e.g. deletion of expired data)	7.1.1c (Alice)
<i>Compliance Check</i>			
F1-18	Request compliance check	Request a compliance check of a cloud provider or cloud user	1.1.1c (Kim), 1.1.3a (Kim), 7.1.1b (Alice), 13.1.1c (Sandra), 18.1.1a (Sandra)
F1-19	Receive compliance check results	Get the results of the compliance check of a cloud provider/cloud service user	1.1.1c (Kim), 7.1.1b (Alice), 18.1.1a (Sandra)
F1-20	Request role obligations	Explore the actor's responsibilities, based on the policy for handling corporate data	13.1.1a (Sandra)
F1-21	Request conformance	Request compliance with policies on the use of confidential data	13.1.1d (Sandra)
F1-22	Summary of actions	Request the actions with respect to policy enforcement and the relevant incidents for a given period of time	8.1.1a (Bob)
F1-23	Navigate through actions	Filter the list of actions with respect to policy enforcement, based on performer and incident	Derived from F1-22
F1-24	Risk notification	Receive notifications on potential risks derived from the policy settings of the cloud provider/cloud service user	8.1.1b (Bob)

7.2 Functionalities for business end users (cloud users)

This section summarises the functionalities, which have been identified for the business end users (cloud users) in the scenarios reflecting the domains of the three business use cases. In principle, this kind of cloud actor can impact the processes on policy management, data governance, compliance check and risk analysis. The functionalities are allocated to these four categories, as shown below.

Table 5 Functionalities for business end users (cloud users)

ID	Functionality	Description	Source scenario(s)
<i>Policy Management</i>			
F2-1	View regulation framework	Explore the provisions and restrictions of the data protection law	3.1.1a (Michael)
F2-2	Request for regulation framework	Search for the appropriate regulation framework governing the execution of a specific application scenario	Derived from F2-1
F2-3	Receive policy notification	Receive notifications on the status of the policy enforcement for personal and corporate data, including policy violations	3.1.1a (Michael), 14.1.1d (Paul)
F2-4	Analyse violation	Track the policy violation data to identify which parties are affected and which personal and/or corporate data are violated and how	3.1.3a (Michael), 3.1.3b (Michael), 14.1.1c (Paul)
F2-5	Edit policy	Create, modify or delete a policy about the use of corporate data and devices	14.1.1b (Paul)
F2-6	View redress actions	Explore the list of recommended actions in case of receiving a policy notification, such as a policy violation	3.1.3b (Michael)
F2-7	Implement redress actions	Select and implement the action(s) to remediate and redress the incident caused the notification alert	Derived from F2-6
F2-8	Inform users	View and submit automatically generated notifications for infringements on the use of corporate data subjects	14.1.1e (Paul)
F2-9	List users	View the list of individual end users associated with a policy on the use of corporate data	Derived from F2-8
<i>Data Governance</i>			
F2-10	View policy settings	Request to explore the fields comprising the user policy on governing the use of personal data	3.1.1a (Michael)
F2-11	Track personal data	Track the reference to the personal data (but not the contents of the personal data) of those involved in the execution of corporate processes	3.1.1b (Michael)
F2-12	Analyse use	Analyse the trace on the use of personal and corporate data with respect to how data is stored by the cloud provider, what data have been collected and when and who accessed this data	Derived from F2-11
F2-13	Request data tracking	Select which personal and corporate data used in the cloud should be tracked	Derived from F2-11
F2-14	Select data	Decide which corporate data can be placed in the cloud	3.1.1a (Michael)
F2-15	Edit data	Correct or delete the personal data used in the cloud	Derived from F2-14
<i>Compliance Check</i>			

D:B-3.1 Use Case Descriptions

ID	Functionality	Description	Source scenario(s)
F2-16	Match data	Match personal and corporate data collected with the terms of the contract established with the cloud provider	3.1.1c (Michael)
F2-17	Negotiate contract	Negotiate the contract terms to establish agreement with the cloud provider	Derived from F2-16
F2-18	Collect data for evidence	Collect data from the cloud as evidence to configure the proper policy enforcement	3.1.1d (Michael)
F2-19	Share evidence	Share results on the evidence collection data with individual cloud users	3.1.1e (Michael)
F2-20	Request compliance check	Check corporate data governance policies with respect to regulation	14.1.1a (Paul)
F2-21	Select processes	Define corporate data governance policy process	Derived from F2-20
F2-22	Report on compliance	Prepare reports on corporate compliance to legislation bodies	14.1.1a (Paul)
<i>Risk Analysis</i>			
F2-23	Perform risk analysis	Define which data will be used for risk assessment and request risk analysis	3.1.2a (Michael)
F2-24	Define risk model	Select which risk analysis model (including configuration thresholds) should be adopted to run risk analysis	Derived from F2-23
F2-25	Define trust model	Select which trust model (including configuration thresholds) should be adopted to run risk analysis	Derived from F2-23
F2-26	Explore cloud providers	Explore the list with the associated cloud providers	Derived from F2-23
F2-27	View risk results	View risk analysis results	3.1.2a (Michael)

7.3 Functionalities for cloud providers

This section summarises the functionalities, which have been identified for the cloud providers in the scenarios reflecting the domains of the three business use cases. In principle, this kind of cloud actor can impact the processes on policy management, data governance, compliance check and risk analysis. The functionalities are allocated to these four categories, as shown below.

Table 6 Functionalities for cloud providers

ID	Functionality	Description	Source scenario(s)
<i>Policy Management</i>			
F3-1	Edit contract	Create, modify or delete a contract about the use of cloud resources	4.1.1a (Peter), 4.1.1b (Peter) 15.1.1b (Roger)
F3-2	Negotiate contract	Negotiate the contract terms to establish agreement with the cloud user	4.1.2a (Peter)
F3-3	Receive policy notification	Receive notifications on the status of the policy enforcement for personal and corporate data, including policy violations	4.1.3a (Peter)

D:B-3.1 Use Case Descriptions

ID	Functionality	Description	Source scenario(s)
F3-4	Define accountability policy	Define the policy with respect to the processes and the data for the cloud provider being accountable	9.1.1a (Charles)
F3-5	View policy notifications	Explore the list of the policy related notifications, which have been generated	11.1.1a (Edgar)
F3-6	Analyse violation	Track the policy violation data to identify which parties are affected, if they have been informed about the violation and which personal and/or corporate data are violated and how	11.1.1a (Edgar)
F3-7	Rank policy notifications	Assess and rank significance of policy violations	11.1.1a (Edgar)
F3-8	Enforce policy	Set a policy into force	15.1.1c (Roger), 19.1.1a (Linda)
F3-9	Submit policy notifications	Generate notifications about policy violations, including the list of notification receivers	15.1.1d (Roger)
<i>Data Governance</i>			
F3-10	Define evidence data	Identify types of records to collect for evidence (i.e. security patches applied to the platform software, code scans and reviews, the backups performed)	9.1.1a (Charles)
F3-11	Select data location	Bind the network and storage resources that are to host personal data and corporate data in the cloud to a particular geographic location	5.1.1a (Bruce)
F3-12	Select legal regime	Bind the network and storage resources that are to host personal data and corporate data in the cloud to a particular legal regime	Derived from F3-11
F3-13	Submit data for evidence	Enable the collection of providers' data as evidence for checking compliance to accountability practices	20.1.1a (Peter) 5.1.1b (Bruce)
F3-14	Share access rights for evidence	Grant access rights to customers and auditors to collect evidence data	Derived from F3-13
F3-15	Collect user feedback	Collect needs and concerns from users to refine policy configuration	15.1.1f (Roger)
F3-16	Respond to user feedback	Decide on actions to address users' concerns and needs	15.1.1f (Roger)
<i>Compliance Check</i>			
F3-17	Request provider status	Request for other cloud providers' configuration	4.1.3a (Peter)
F3-18	Publish provider status	Publish the own configuration of cloud provider	Derived from F3-17
F3-19	Request compliance check	Request the compliance of other cloud providers, through seeking guarantees	4.1.4a (Peter), 15.1.1a(Roger)

D:B-3.1 Use Case Descriptions

ID	Functionality	Description	Source scenario(s)
F3-20	Manage audits	Manage the auditing system	5.1.1a (Bruce) 5.1.1b (Bruce)
F3-21	Request accountability check	Check providers' procedures and policies to regulation with respect to accountability compliance	9.1.1a (Charles)
<i>Risk Analysis</i>			
F3-22	Define data types	Define type of personal data to be used for risk analysis	10.1.1a (David)
F3-23	Define purpose of use	Define purpose of processing personal data for risk analysis	10.1.1a (David)
F3-24	Define access rights	Defines roles accessing personal data for risk analysis	10.1.1a (David)
F3-25	Define risk model	Select which risk analysis model (including configuration thresholds) should be adopted to run risk analysis	10.1.1a (David)
F3-26	Define trust model	Select which trust model (including configuration thresholds) should be adopted to run risk analysis	10.1.1a (David)
F3-27	Perform risk analysis	Request to run risk analysis	10.1.1a (David)
F3-28	Perform parallel risk analysis	Run risk analysis for selected providers	15.1.1e (Roger)
F3-29	Explore cloud providers	Explore the list with the associated cloud providers	Derived from F3-28
F3-30	View risk results	View results of risk analysis	10.1.1a (David)

7.4 Functionalities for cloud auditors

This section summarises the functionalities, which have been identified for the cloud auditors in the scenarios reflecting the domains of the three business use cases. In principle, this kind of cloud actor can impact the process on compliance check. The functionalities are allocated to this category, as shown below.

Table 7 Functionalities for cloud auditors

ID	Functionality	Description	Source scenario(s)
<i>Compliance Check</i>			
F4-1	Collect data for evidence	Collect data from the cloud, including corporate incident handling procedures, as evidence that accountability practices are being followed	6.1.1a (Leslie), 12.1.1a (Frank), 16.1.1a (Michael) 17.1.1a (John)
F4-2	Accountability support	Report on the results on accountability checks, provide recommendations towards accountability compliance and legal guidance for redress	6.1.1b (Leslie), 12.1.1a (Frank), 16.1.1a (Michael), 17.1.1b (John)
F4-3	Certify accountability	Certify compliance with data protection legislation	Derived from F4-2
F4-4	View policy notifications	Explore the list of the policy	12.1.1a (Frank),

D:B-3.1 Use Case Descriptions

ID	Functionality	Description	Source scenario(s)
		related notifications, which have been generated, in order to assess their severity	17.1.1b (John)
F4-5	Verify risk analysis	Review process on risk assessment	12.1.1a (Frank)
F4-6	Verify mitigation actions	Check privacy impact assessment and mitigation plan and review on remediation and redress actions	12.1.1a (Frank), 12.1.1b (Frank), 16.1.1a (Michael)
F4-7	Accountability alert	Generate alerts and notifications in case that a cloud actor is not accountable	12.1.1b (Frank), 16.1.1a (Michael)
F4-8	List accountability actions	View the list of responsibilities for the involved cloud actors, associated with liabilities	12.1.1b (Frank)
F4-9	Suggest compensation	Decide on sanctions in case of infringement	17.1.1b (John)
F4-10	Revoke certification	Revoke certificates from cloud actors	Derived from F4-7

8 Conclusions

This deliverable provides an initial description of the three different business use cases, which will be used to demonstrate the A4Cloud accountability approach. The business use cases have been described in terms of as-is and to-be scenarios, and analysed with respect to accountability relationships and high-level functionalities. As has been shown, the three business use cases are quite different and they complement each other. The main features characterizing the first business use case ("Health care services in the cloud") is the processing and storage of sensitive personal data in the cloud. The second business use case ("Cloud-based ERP software enabled with 3rd party extensions") deals with the problem of respecting end users' privacy preferences throughout a chain of service providers in the cloud. The third and last business use case ("Rights and relevant obligations in a multi-tenant cloud scenario") analyses the problems associated with BYOD and data governance in cloud computing.

The main contribution of this work package is the to-be scenarios. They will serve as input to several other work packages; in particular the ones in Stream C, which will define and develop a framework of concepts for A4Cloud, and stream D, which will provide a set of tools for accountability. The to-be scenarios will also provide a foundation for the dissemination activities in Stream A and for communicating with stakeholders during the elicitation activities in Stream B.

This deliverable also provides a set of accountability relationships (Section 6). These relationships will eventually be integrated in the collection of requirements that are created in A4Cloud, which purpose is to ensure a smooth way of communicating the (sometimes changing) requirements to the work packages that need them. In addition, we provide a high-level functional analysis (Section 7), which identifies an initial set of functionalities that cloud actors will need, in the three distinct domains. The set of functionalities will serve as input to a number of other work packages that are developing the accountability concepts, mechanisms and tools. The set of functionalities has already been adopted by WP:C-7, which will use it as a basis for developing Human Computer Interaction (HCI) principles and guidelines for the tools that are to be developed in A4Cloud and by WP:C-8, which have started to analyse the functionalities in detail (creating sequence diagrams) in order to determine what types of evidences that will be required to achieve accountability in the cloud.

In the next step, the to-be scenarios, and the associated list of functionalities, will be analysed further, in order to assess their feasibility with respect to what the conceptual and technical work packages in Stream C and Stream D will achieve. The business use case descriptions will be iteratively updated and refined based on feedback and findings from the other work packages in the project. Subsequent iterations will be elaborated in more detail, eventually allowing one (or more) of the business use cases to be instantiated in WP:D-7.

Finally, we would like to point out that the legal analysis of the roles in the different business use cases (in particular regarding who are the controllers and processors of personal data) is based on our interpretation of Directive 95/46/EC. Since the directive is being reformed, we will redo this analysis at a later stage in the project, taking the proposed draft regulation on data protection into account.

References

- [1] P. M. Timothy Grance, *The NIST Definition of Cloud Computing*. 2011.
- [2] Siani Pearson (editor), “MSC-2.1 Scoping report and initial glossary,” A4Cloud Milestone Report, Dec. 2012.
- [3] Nils Brede Moe (editor), “Stakeholder Workshop 1 Results (Initial Requirements),” A4Cloud Deliverable, Mar. 2013.
- [4] M. Fowler, *UML Distilled: A Brief Guide to the Standard Object Modeling Language (3rd Edition)*, 3rd ed. Addison-Wesley Professional, 2003.
- [5] Siani Pearson and Massimo Felici (editors), “MSC-2.2 Initial Conceptual Framework,” A4Cloud Milestone Report, Mar. 2013.
- [6] “EU Directive 95/46/EC - The Data Protection Directive.”
- [7] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, *NIST Cloud Computing Reference Architecture*. 2011.
- [8] Paul Simmonds, Chris Rezek, and Archie Reed, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,” Cloud Security Alliance, 3.0, 2011.
- [9] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, “Cloud Computing Synopsis and Recommendations,” National Institute of Standards and Technology, 800-146, May 2012.
- [10] Cloud Computing Use Case Discussion Group, “Cloud Computing Use Cases White Paper.” Jul-2010.
- [11] Siani Pearson and Massimo Felici (editors), “MSC-2.3,” A4Cloud Milestone Report (work in progress).
- [12] QMUL and Tilburg, “MSC-5.1 A4Cloud Accountability Legal Scoping Paper,” A4Cloud Milestone Report, Dec. 2012.
- [13] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, “Wireless Sensor Networks for Healthcare,” *Proc. Ieee*, vol. 98, no. 11, pp. 1947–1960, Nov. 2010.
- [14] J. Biswas, J. Maniyeri, K. Gopalakrishnan, L. Shue, P. J. Eugene, H. N. Palit, Foo Yong Siang, Lau Lik Seng, and Li Xiaorong, “Processing of wearable sensor data on the cloud - a step towards scaling of continuous monitoring of health and well-being,” 2010, pp. 3860–3863.
- [15] QMUL and Tilburg, “MSC-5.2 The Role of Contracts,” A4Cloud Milestone Report, May 2013.
- [16] C. Dwork and M. Naor, “On the Difficulties of Disclosure Prevention in Statistical Databases or The Case for Differential Privacy,” in *Journal of Privacy and Confidentiality*, vol. 2, 2010, pp. 93–107.
- [17] “Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data.”
- [18] Matthijs Koot, *Measuring and Predicting Anonymity*. 2012.
- [19] A. Narayanan and V. Shmatikov, “Myths and fallacies of ‘Personally Identifiable Information’,” *Commun Acm*, vol. 53, no. 6, pp. 24–26, Jun. 2010.
- [20] “Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing.”
- [21] “Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’.”

Appendix A An A4Cloud Taxonomy of Stakeholders

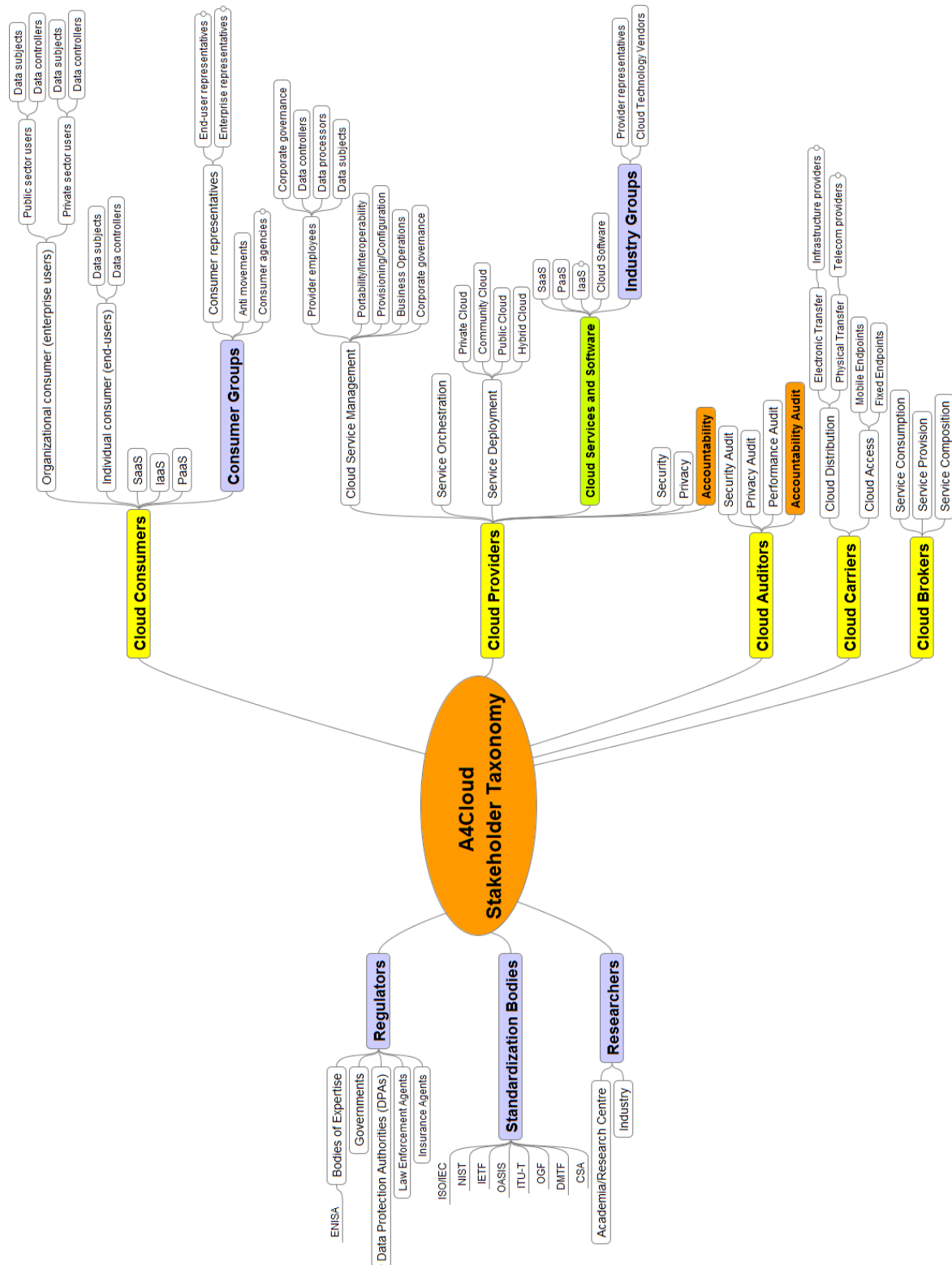


Figure 8 An A4Cloud taxonomy of stakeholders

Appendix B Data Controllers and Processors

Figure 9 is based on Article 29 Working Party Opinion WP169 on controller/processor [21].

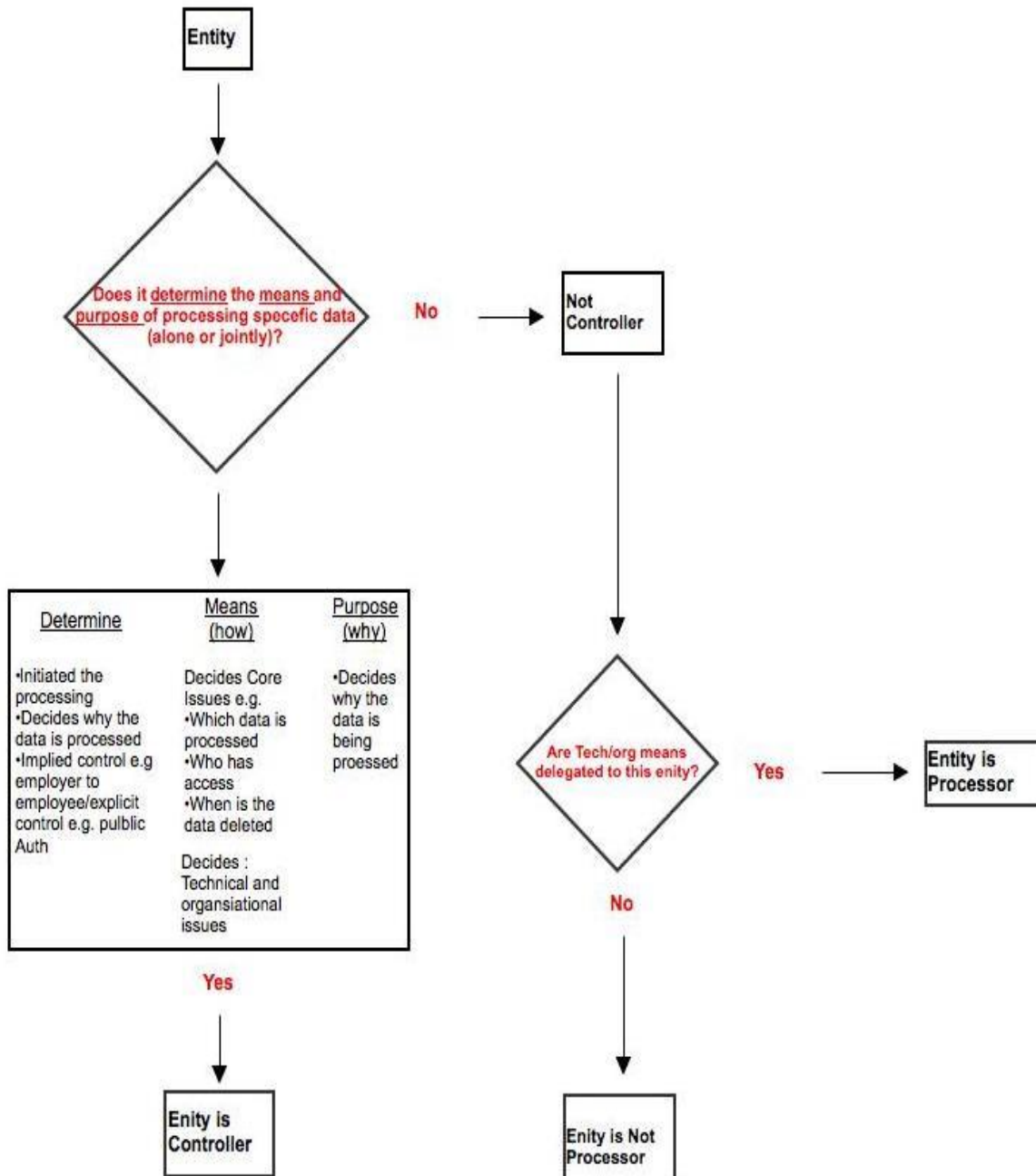


Figure 9 Controllers and processors under the Directive 95/46/EC

Appendix C Scenarios for Business Use Case 1

In order to relate relevant accountability issues to potential stakeholders of the system outlined in Figure 1, we will use a set of personas and their perceived challenges related to care and the use of such a system.

Individual end users **Kim** is one of the elderly living in Trondheim and who is enrolled in the Ageing Well program. **Sandra** is Kim's daughter.

(Representatives of) business end users **Michael** is a privacy officer at the IT department at St Olav hospital.

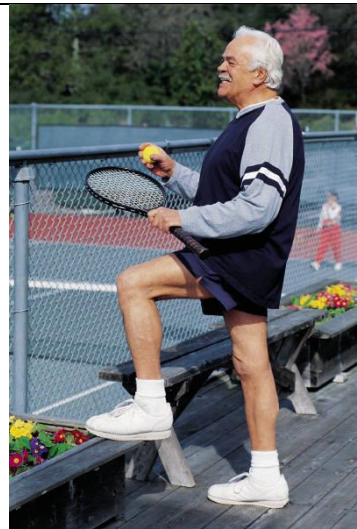
Cloud service providers **Peter** is a software architect in the Norwegian software company delivering the MedNet platform to St Olav hospital (Cloud z).

Bruce is an infrastructure manager at the cloud provider delivering the sensor data storage and back-up services (Cloud y).




Regulators/auditors **Leslie** is a senior advisor at the Norwegian Data Authority

Scenario 1: Kim



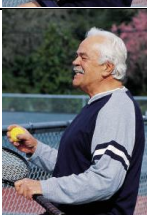
As-is scenario 1.1: Kim is worried about data collection and storage

	<p>Actor: Kim Kim (72 years) is a patient in the Ageing Well program. He is a healthy retired person who would like to maintain an active lifestyle as long as possible, however, during the past months he has been suffering from severe dizziness. Diagnosing a balance disorder is difficult and after being subject to a thorough physical examination by his GP he has enrolled in the Ageing Well program. Data from an oximeter, sensors monitoring his heart rate, blood pressure, pulse, temperature and movements will be combined with data from his medical history in order to help make a diagnosis. To make a diagnosis Kim will be monitored for one week at a time, followed by an additional examination by his GP.</p> <p>Role in the cloud ecosystem: Individual end user</p> <p>Computer experience: Kim has rudimentary computer skills.</p>	<p>Problem scenario told by Kim: Kim has agreed to participate in the Ageing Well program. However, he does not like the idea of someone tracking his movements, even though he knows this is not the intention of the program. He would like to know what data will be collected from the sensors and who will have access to it. Kim has also been informed that his data will be used for research; however he doesn't understand what this means. Kim signed an agreement when enrolling in the program, but he does not really understand the terms and conditions that he has agreed to.</p> <p>Kim's main accountability concerns:</p> <ul style="list-style-type: none"> • Privacy • Unclear contract terms • Data minimization
--	--	--

To-be scenario 1.1.1: Kim gets an increased understanding and overview over the collection and usage of sensor data


	<p>Scenario 1.1.1a: viewing the data policies Kim uses a tool to view the data policies for his personal data. Kim is able to see what kind of sensor data that will be collected and for what purpose, who will be able to access it and how long the data will be stored.</p>
	<p>Scenario 1.1.1b: checking what has happened to his data Kim uses a tool that provides him with a report of what data has been collected from him so far. The report also includes information on who has accessed the data (and for what purposes), where the data is currently being stored and its expiry date.</p>
	<p>Scenario 1.1.1c: verifying compliance Kim uses a tool that gives Kim an instant confirmation of whether his data has been used in accordance to what has been agreed, and in accordance to legal requirements.</p>

To-be scenario 1.1.2: Kim actively controls the collection and usage of his own data

	<p>Scenario 1.1.2a: Kim changes his privacy preferences Kim still does not like the thought of being tracked. He uses a tool that allows him to change his preferences regarding what kind of sensor data will be collected. Kim disables the system's ability to collect any kind of data related to his position (i.e. data from the movement sensor).</p>
	<p>Scenario 1.1.2b: Kim changes who can access the data Kim does not want his data to be used for any other purposes than diagnosis of his dizziness. He uses a tool to remove the possibilities for research organisations (and other actors such as insurance companies) to access any information that is related to himself.</p>
	<p>Scenario 1.1.2c: Kim requests data deletion (Follow up on Scenario 1.1.2b) Kim uses a tool to request that all data that previously has been collected for research purposes is deleted.</p>


To-be scenario 1.1.3: Kim withdraws from the Ageing Well program

After being part of the Ageing Well program for two weeks, a diagnosis has been made and the treatment (consisting of medication combined with daily exercises) is started. Every fourth month he is monitored for six days to understand the effect of the treatment. After a year, Kim feels much better, which is confirmed by the data. Kim decides to leave the Ageing Well program.


	<p>Scenario 1.1.3a: Kim confirms that personal data has been deleted Kim has left the program; however, he suspects that the large amount of personal data that has been collected about him is still "out there". The contract that he signed stated that all personal data is to be deleted no later than 90 days after program termination. Kim uses a tool to confirm that all the personal data that has been collected in the Ageing Well program has been deleted within the time frame stated in the agreement.</p>
---	---

Scenario 2: Sandra

As-is scenario 2.1: Sandra uploads information to the Ageing Well program


	<p>Actor: Sandra Sandra is 39 years old, working as an accountant, she is active on social media, owns a smartphone and several other IT devices. Sandra is Kim's daughter. Kim is a patient in the Ageing Well program.</p> <p>Role in the cloud ecosystem: Individual end user</p> <p>Computer experience: She is skilled</p>	<p>Problem scenario told by Sandra: Sandra has enrolled in the Ageing Well program, as a relative of Kim. Her main obligations are to support Kim in his daily training and to make sure that he is motivated to participate in the program. Since her office is located close to Kim's home, she takes a daily walk with her father during her lunch breaks.</p> <p>Sandra has been provided with a user account in the Ageing Well program, which allows her to upload information about Kim's physical activity¹⁶. This is done through an app on her smartphone, which allows her to register what kind of activity Kim has performed, the date and time, and the duration of the activity.</p> <p>Sandra is very concerned about privacy and wants to make sure that the registration of daily exercises does not involve any tracking of either her or Kim's movements</p> <p>Sandra's main accountability concerns:</p> <ul style="list-style-type: none"> • Kim's privacy • Her own privacy
--	---	---

To-be scenario 2.1.1: Sandra

	<p>Scenario 2.1.1a: Sandra uploads data about Kim Sandra uses an app on her smartphone to collect and upload information about Kim's daily exercises to the Ageing Well program (date and time, type of activity, duration of activity). Since Kim has told Sandra that he dislikes being tracked (Scenario 1.1.2a), Sandra has disabled the app's ability to collect any information related to Kim's position¹⁷.</p>
---	---


¹⁶ Kim's agreement with the Ageing Well program states that relatives who enroll in the program will have access to the patient's account, hence giving them consent to use his personal data.

¹⁷ If Sandra does not limit the tracking option, then data uploaded about Kim could be uploaded including details of his location etc. since Kim has given Sandra consent to upload personal data relating to him.




	<p>Scenario 2.1.1b: Sandra controls her own personal data Sandra is able to set data policies associated with all her personal data that she provides. She makes sure that no position data (related to her) will be collected in the Ageing Well program.</p>
---	--

Scenario 3: Michael



As-is scenario 3.1: Michael is responsible for the collection of personal data

	<p>Actor: Michael Michael (49 years) is a privacy officer at the IT department at St Olav hospital. His primary job responsibility as a privacy officer is to control how personal data collected in the Ageing Well program will be managed and used.</p> <p>Role in the Cloud ecosystem: Cloud service user</p> <p>Computer experience: He is skilled.</p>	<p>Problem scenario told by Michael: Several of the patients and their relatives in the Ageing Well program have started asking him about the data that is being collected by the sensors. He needs to assure them that their privacy preferences have been (and are being) enforced.</p> <p>Michael will also need to be able to check that the various service providers have complied with their contracts when processing data (as these may be more restrictive than the elderly's privacy preferences). He furthermore needs to verify that applicable law has been complied with.</p> <p>In addition, Michael's manager has asked him to clarify the possible consequence for St Olav hospital if any of the terms in the hospitals contract with the MedNet platform service provider is broken (for example if the elderly's' preferences regarding personal data are violated, either by MedNet or by any of the other cloud service providers involved in the service provision chain).</p> <p>Michael's main accountability concerns:</p> <ul style="list-style-type: none"> • Individual end users' privacy policies • Risk management • Compliance with applicable data protection regulation
--	--	---


To-be scenario 3.1.1: Michael verifies compliance with contracts, laws and preferences

	<p>Scenario 3.1.1a: Michael sets data policies Based on the individual end users' privacy preferences, as well as the restrictions implied by applicable law, Michael uses a tool that allows him to set data policies for all the data that will be collected and processed in the Ageing Well program. Policies can be set both on the general level (affecting data collected from all data subjects) as well as on individual levels (affecting data collected from individual end users)</p>
	<p>Scenario 3.1.1b: Michael tracks the collection and processing of data Michael uses a tool that allows him to track personal data in the cloud, showing what type of data has been collected, where it has been stored and who has had access to it. Even though Michael is not able to view personal data belonging to individuals, he can still track its usage in the Cloud.</p>
	<p>Scenario 3.1.1c: Michael checks that the service provider have complied with their contracts The tool outlined in Scenario 3.1.1b allowed Michael to track the personal data in the cloud. The same tool allows him to compare the track record with the contract terms that St Olav hospital and the MedNet platform provider have agreed upon.</p>



D:B-3.1 Use Case Descriptions

	<p>Scenario 3.1.1d: Michael collects evidence about the correct enforcement of privacy policies</p> <p>The tool outlined in Scenario 3.1.1b allowed Michael to track the personal data in the cloud. The same tool allows him to compare the track record with the data subject's privacy preferences and to gather evidence that these have been enforced (for example snippets of log files which have been signed by a trusted third party).</p>
	<p>Scenario 3.1.1e: Michael presents the evidence to the elderly</p> <p>The tool outlined in Scenario 3.1.1d allows Michael to compile and print a report over the types of collected personal data belonging to a particular data subject.</p>

To-be scenario 3.1.2: Michael performs a risk evaluation


	<p>Scenario 3.1.2a: Michael identify risks in the service provisioning chain</p> <p>Michael uses a tool that lets him identify the risks associated with using the MedNet platform in the Ageing Well program. The tool takes as input what kind of data that will be collected (personal and medical data, etc.) and how it will be used, and combines this with a trustworthiness analysis of the complete chain of providers involved in the delivery of the MedNet platform service.</p>
---	---

To-be scenario 3.1.3: Michael manages contract breaches



	<p>Scenario 3.1.3a: Michael is notified of a policy violation</p> <p>Michael uses a tool that keeps track of any policy violation that may occur and that notifies him of potential contract breaches.</p>
	<p>Scenario 3.1.3b: Michael responds to a policy violation</p> <p>Michael uses a tool to investigate which parties were affected by the policy violation and which actions need to be taken to mitigate the incident and redress the affected parties.</p>

Scenario 4: Peter


As-is scenario 4.1: Peter is responsible for procurement of cloud services from sub providers

	<p>Actor: Peter Peter is a senior system architect at the Norwegian company delivering the MedNet platform to St Olav hospital. He is responsible for the overall architecture of the platform as well as for compliance with applicable law.</p> <p>Role in the cloud ecosystem: Cloud service provider (Cloud z) and cloud user (Cloud x, Cloud y)</p> <p>Computer experience: He is an expert.</p>	<p>Problem scenario told by Peter: Peter needs to make sure that the obligations in the contract with St Olav hospital are fulfilled when outsourcing parts of the functionality of the MedNet platform to 3rd part cloud service providers. In particular he needs to verify that the collection and processing of personal and medical sensor data by Cloud x and Cloud y is done in adherence to the associated data policies.</p> <p>Peter's main accountability concerns:</p> <ul style="list-style-type: none"> • Compliance with contractual terms • The trustworthiness of sub providers • Compliance with Norwegian law
---	--	--

To-be scenario 4.1.1: Peter drafts contract terms


	<p>Scenario 4.1.1a: Peter drafts the contracts with St Olav hospital Acting as a cloud provider, Peter uses a tool, which supports him in the process of establishing the contracts with St Olav Hospital. The contract will include a number of restrictions related to data collection and processing that the MedNet platform needs to adhere to.</p>
	<p>Scenario 4.1.1b: Peter drafts the contracts with the sub providers Acting as a cloud user, Peter uses a tool, which supports him in the process of establishing the contracts with Cloud x and Cloud y. The tools helps him to establish contracts that are in line with the existing contract St Olav Hospital</p>

To-be scenario 4.1.2: Peter renegotiates a contract


	<p>Scenario 4.1.2a: Peter renegotiates a contract Peter uses a tool to renegotiate St Olav hospital's contract with the Norwegian company delivering the MedNet platform. The tools allows him to propose changes to the existing contract terms, such as more stringent restrictions on where the data is being stored or guarantees on how long it will take before data will be deleted after the deletion has been requested¹⁸.</p>
---	---

¹⁸ The tool allows mutual rights and obligations to be managed. It does not reflect commercial realities (such as effects on budgets or commercial interests) or internal procurement procedures.

To-be scenario 4.1.3: Peter audits the service provisioning chain

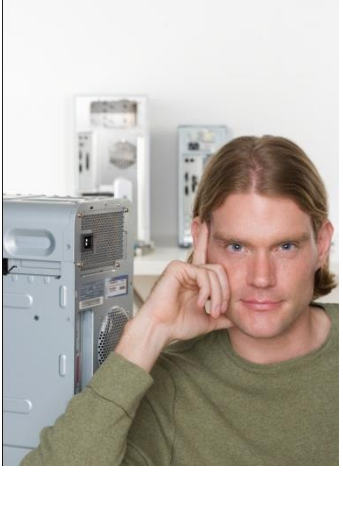
	<p>Scenario 4.1.3a: Peter audits the sub providers Peter uses a tool that allows him to audit cloud infrastructures. The tool will provide him with an overview over the current configuration of Cloud x and Cloud y, and will notify him of any policy violations that are detected.</p>
---	--

To-be scenario 4.1.4: Peter searches for alternative cloud providers

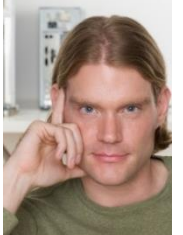
	<p>Scenario 4.1.4a: Peter searches for alternative sub providers By using a tool for service orchestration and composition, Peter is able to find an alternative cloud provider who can deliver the same functionality as Cloud y, but that can give stronger guarantees on the collection and storage of personal data (for example that it will always be stored in, and never transferred outside, one of their existing datacentre located in northern Norway). This information is useful both as a basis for renegotiating the contract with Cloud y, or as a part of a future migration plan from Cloud y to the alternative provider</p>
---	--


Scenario 5: Bruce

As-is scenario 5.1: Bruce

	<p>Actor: Bruce Bruce is an infrastructure manager at Cloud provider y, which is delivering the data storage and back-up services to the MedNet platform.</p> <p>Role in the cloud ecosystem: Cloud provider</p> <p>Computer experience: He is an expert.</p>	<p>Problem scenario told by Bruce: Several of the existing customers of Cloud provider y (for example the Norwegian company that delivers the MedNet platform) have asked for more transparency on how provider y deals with the customer data. Bruce currently does not have anything to offer them; all he can do is to refer to the contract terms that state that all the customer data will be stored in one of their datacentres in Europe.</p> <p>Bruce's main accountability concerns:</p> <ul style="list-style-type: none"> Assuring customers that data policies are adhered to
---	--	--

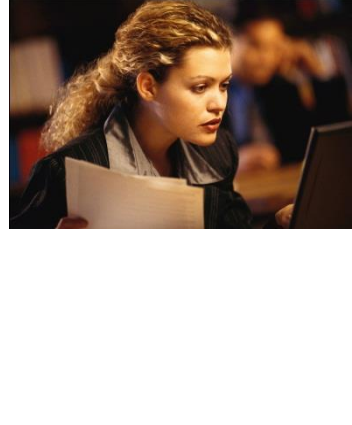
To-be scenario 5.1.1: Bruce

	<p>Scenario 5.1.1a: Bruce enables transparency in the datacentres Bruce installs and deploys an audit agent system, which allows him to audit the cloud infrastructure. The agent system makes it possible to track the customers' data across the cloud, verifying where it has been transferred; who's had access to it and in what data centre it is currently being stored.</p>
---	---

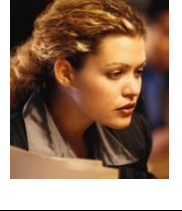
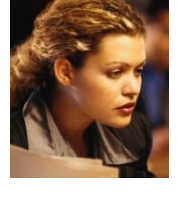
	<p>Scenario 5.1.1b: Bruce enables customer control in their datacentres Bruce uses a tool that allows Cloud y's customer to export relevant tracking data produced by the audit agent system described in Scenario 5.1.1.a.</p>
---	---

Scenario 6: Leslie

As-is scenario 6.1: Leslie

	<p>Actor: Leslie Leslie is a senior advisor at the Norwegian Data Protection Authority.</p> <p>Role in the cloud ecosystem: Regulator</p> <p>Computer experience: She is skilled.</p>	<p>Problem scenario told by Lee: Leslie has been contacted by Peter, who is a system architect at the Norwegian company delivering the MedNet platform. Peter told her that he recently discovered that the customer support and maintenance division of Cloud x is located in India. Even though provider x stores all the collected sensor data in one of their data centres in Norway, they are not able to prove that the support data that is being processed by the Indian division does not include (unencrypted) sensor data. Peter suspects this may be a potential violation of applicable law and has asked Leslie to investigate this further.</p>
--	---	--

To-be scenario 6.1.1: Leslie

	<p>Scenario 6.1.1a: Leslie gathers evidence Leslie uses a tool that allows her to review evidences of the collection and processing of sensor data by Cloud provider x</p>
	<p>Scenario 6.1.1b: Leslie helps Peter file a complaint Leslie makes Peter aware of a tool that he can use in order to file a complaint against Cloud provider x. Leslie supports Peter through the process and provides him with legal guidance.</p>

Appendix D Scenarios for Business Use Case 2


In order to relate relevant accountability issues to potential stakeholders of the system outlined in Figure 4 we will use a set of personas and their perceived challenges related to care and the use of the cloud services described here.

Individual end user (Representative of a) Cloud user (primary service provider)	Alice is a teacher and customer of the MarchéAzur stores. Bob is a business analyst for MarchéAzur.
Cloud providers	Charles, David, Edgar work either as developers or system administrators for the different cloud service providers involved in this business case.
Regulators/auditors	Frank is a senior advisor at the CNIL (French Data Protection Authority)


Scenario 7: Alice

Alice would like to have simple dashboard informing her about which data is stored and processed by the MarchéAzur.



As-is scenario 7.1:

	<p>Actor: Alice is 32 years old, working as a teacher, she is active on social media, owns a smartphone and a PC.</p> <p>Role in the cloud ecosystem: Individual end user.</p> <p>Computer experience: She is skilled</p>	<p>Problem Scenario told by Alice: Alice, an individual end user, has subscribed to the MarchéAzur loyalty program. As she shops in its stores, she receives offers and discount coupons on her smartphone. As a counterpart she agreed to allow MarchéAzur to collect her personal data and shopping habits. She was not informed about the actual risks to her privacy, or whether MarchéAzur had been through any process that ensured its accountability w.r.t data protection. Moreover, there is no existing functionality of the application that provides her possibility to ensure that the privacy policy is fulfilled (e.g. collected data related to shopping history is deleted). Sometimes Alice also receives advertisement from MarchéAzur partners, or requests to answer surveys, among other things for which she is not so sure she has agreed to. She wonders why it is not possible to assure that her choice has been correctly taken into account.</p>
--	--	---

To-be scenario 7.1.1:

	<p>Scenario 7.1.1a: Alice would like to learn what information the supermarket has collected when she was using the application and also making shopping. She opens a simple dashboard providing her insight into the data collected by the supermarket throughout the last day, week, month, year and since the subscription to the fidelity program. She can also access the additional information like where her personal data is stored and when it will be deleted according to the retention period that MarchéAzur stated in the terms of use for their application. She is also able to exercise her rights such as to access, correct, and remove data</p>
---	---


D:B-3.1 Use Case Descriptions

	<p>from the cloud. She sees that she currently gives MarchéAzur and 3rd party software companies access to data on groceries, healthcare articles and clothing. Re-evaluating her needs for offers she decides that she does not want offers about groceries, she revokes their access rights to this. She also marks that all previously gathered information about groceries is to be deleted. The app reports that this shall be done.</p>
	<p>Scenario 7.1.1b: Alice receives an offer for a grocery item. She clicks on its properties to request justification from MarchéAzur, as well as information about whether data retention period has been observed, thanks to receiving prompt and trusted answers from the service. MarchéAzur, in the role of data controller, will be able to use accountability enforcement tools to recover evidence of correct data handling.</p>
	<p>Scenario 7.1.1c: As she opens the application, Alice receives a notification informing that her shopping records from two years ago were deleted. That action was performed according to the privacy policy which stated that the retention period for the shopping history records is two years.</p>



Scenario 8: Bob

Business user wishes more automation in obligation execution and compliance assertion.

As-is scenario 8.1:

	<p>Actor: Bob is 40 years old, working as a business analyst at MarchéAzur, he analyses customer behaviour and runs data mining applications on personal data collected by the company.</p>	<p>Problem Scenario told by Bob: His daily work consists in creating different offers that will maximize profit from the analysis of the on premise ERP combined with the data mined in the cloud based extensions provided by Check-it out. As he creates new offers to be sent out to customers the system may automatically consider some privacy preferences, but other obligations are rather executed manually, possibly leading to human errors and non-compliance. Bob finds it is hard to verify if obligations were fulfilled, it is too time consuming, as he is usually already under a lot of pressure for sales results. In order to reach his sales objectives, Bob is encouraged to interact as much as possible with MarchéAzur suppliers, capitalizing on the data collected from its customers. He may then further provide personal data to suppliers to optimize offers and get additional rebates – He simply hopes the access controls concerning the customers privacy preferences really work – anyway he has no visibility on how much data has been released or where it was stored. Bob and his legal team lack tool support when establishing new contracts with software providers in the cloud such as Check-it-out, in order to ensure that terms cover all responsibilities and accountability issues, not currently clearly covered by regulations.</p>
	<p>Role in the cloud ecosystem: Business end user.</p> <p>Computer experience: He is expert.</p>	


To-be scenario 8.1.1:

	<p>Scenario 8.1.1a: During an internal audit, Bob accesses the interface for an accountability evidence management tool. He selects a period (e.g. last 6 months) and the tool generates a report regarding the operations performed (data deletion), and further information related to execution of that processes (automatic/manual trigger, consistency post-checks, incidents that happened during performing that actions – aborted, delayed, etc.).</p>
	<p>Scenario 8.1.1b: Bob and the legal team at MarchéAzur receive a notification from the SaaS provider (Check-it-out) about changes in the terms of use for their service. Bob access a tool to update the model for the service. The tool indicated what the potential risks are the impact to accountability, based on different models from its knowledge base.</p>


Scenario 9: Charles

The PaaS solution offers access to raw log files off the applications deployed in the cloud.

As-is scenario 9.1:

	<p>Actor: Charles is 28 years old, working as a cloud developer responsible for part of the services provided by the PaaSPort company, he maintains the cloud based services hosting the Check-it-out solution for retailers.</p> <p>Role in the cloud ecosystem: Developer.</p> <p>Computer experience: He is an expert</p>	<p>Problem Scenario told by Charles: Although the regular audits of the multi-tenant PaaSPort services have successfully been conducted, the continuously new software being deployed there may lead to new compliance challenges that Charles currently cannot answer to. Developers of these software extensions asked for tools to automate compliance checking or to have more transparency on how the platform is dealing with personal and business sensitive data collected from MarchéAzur customers, but all Charles can do is to offer access to raw log files of the applications deployed in his cloud. Moreover, his company is considering further outsourcing of the high performance database services, which can bring additional compliance issues.</p>
--	--	---

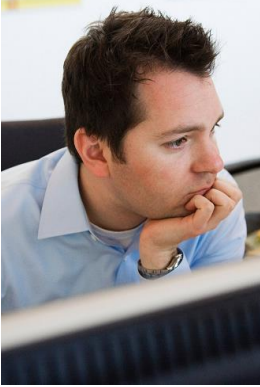
To-be scenario 9.1.1:

	<p>Scenario 9.1.1a: In order to demonstrate that security best practices are in place, Charles uses a policy configuration and enforcement tool. He defines an accountability policy in a machine readable format. The policy takes into account the cloud ecosystem and it is appropriated to the kind of data the multiple tenants are processing in the platform. The policy tells the enforcement system what evidence is to be recorded, for instance, security patches applied to the platform software, code scans and reviews, the backups performed. Later, to check the compliance with the defined policies, Charles can use audit tool to ensure that the mechanisms were correctly enforced.</p>
---	--


Scenario 10: David

Independent software vendor does not allow for the customers to check that their credit card information is deleted afterwards; external audits that are assuring that this obligation is put in place are time-consuming and expensive.

As-is scenario 10.1:

	<p>Actor: David is 25 years old, working as a mobile and cloud application developer at Check-it-out.</p> <p>Role in the Cloud ecosystem: Developer.</p> <p>Computer experience: He is an expert</p>	<p>Problem Scenario told by David: David develops the analytics solution using the PaaS tools from PaaSPort to deliver the data mining and control how offers are sent to the retailer company customers. He is working on new functionality to aggregate more data concerning the customer location and shopping habits. He does not have time to check what will be the impact to the compliance of the software to each customer's privacy agreements with MarchéAzur and other clients of Check-it-out, neither the risks for personal data protection. He foresees some time consuming and expensive compliance audit coming on by the CNIL.</p>
---	---	--


To-be scenario 10.1.1:

	<p>Scenario 10.1.1a: David opens the tool for privacy impact assessments. He updates the characteristics of the personal data processing his service will perform as well as purposes and the roles of the involved actors. The tool uses a risk and trust models to identify what the risks are for the given configuration and environment.</p>
--	--


Scenario 11: Edgar

As-is scenario 11.1:

The infrastructure-as-a-service provider needs to properly notify stakeholders about security breaches and other kinds of security incidents on his services.

	<p>Actor: Edgar is 42 years old and is working as cloud infrastructure administrator. His main responsibility is to administrate the operations of InfraRed infrastructure.</p> <p>Role in the cloud ecosystem: Administrator.</p> <p>Computer experience: He is an expert.</p>	<p>Problem Scenario told by Edgar: It is hard to correctly inform stakeholders about intrusions in the cloud infrastructure. Data subjects are spread across multiple tenants and systems using the infrastructure. There are many difficulties to investigate incidents and the information provided by logs is not always reliable and consistent.</p>
---	--	---


To-be scenario 11.1.1:

	<p>Scenario 11.1.1a: Edgar opens a plug-in for assessment of policy violations. He assesses the significance of the latest policy violations detected, and indicated the relevant stakeholders, who receive appropriate notifications.</p>
---	---

Scenario 12: Frank

As-is scenario 12.1:

The national data protection authority lacks tools to support its activities concerning the growing number of complaints concerning cloud services.

	<p>Actor: Frank is 55 years old has a large experience in the Audit of IT systems.</p> <p>Role in the cloud ecosystem: Data Protection Officer</p> <p>Computer experience: He is expert.</p>	<p>Problem Scenario told by Frank: After some complaints by end users, Frank was entitled with the mission to audit MarchéAzur and its business partner services and infrastructures in order to make sure regulations and data subject rights are being observed. However, the cloud is a new and complex paradigm, and tool support is lacking to help Frank on the multiple facets of the tasks.</p>
--	---	--

To-be scenario 12.1.1:

	<p>Scenario 12.1.1a: Frank will be able to use some solutions from the A4Cloud tool set. He will be able to evaluate policy violations, to have facilitated access to collected evidences, and to verify whether the necessary risk and privacy impact assessments were correctly conducted and mitigation plans were put in place.</p>
	<p>Scenario 12.1.1b: For each case, Frank can use a computer tool to identify responsibilities and liabilities, and to provide proper notification to the different stakeholders involved in the cloud service ecosystem.</p>

Appendix E Scenarios for Business Use Case 3

Business Productivity Cloud Applications

As-Is Scenarios for (1) an employer enterprise ecosystem and its business productivity cloud applications. Sandra accesses business productivity cloud applications provided by her employer enterprise ecosystem. Figure 10 highlights the interaction between business and personal data flows, which are a concern for the employer enterprise ecosystem and its business productivity cloud applications. Other actors involved in the scenario are the Cloud Service Provider (SaaS) and the Cloud Infrastructure Provider (IaaS). Their main concerns are to comply with end user requirements as well as current legislation on data protection.

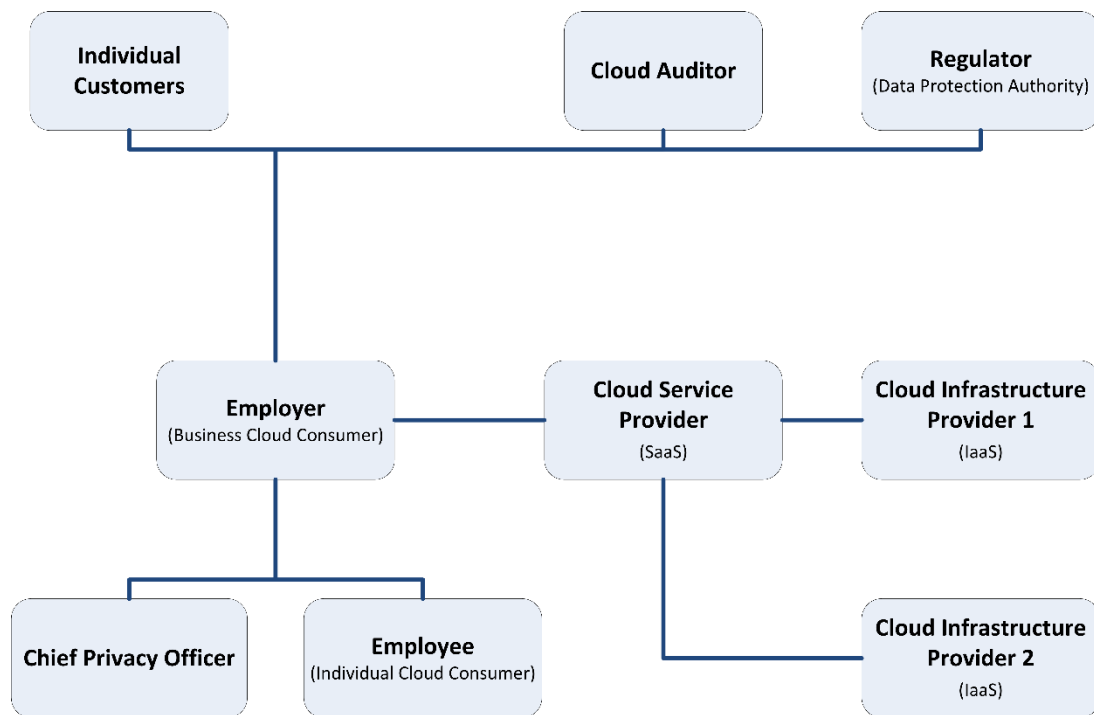




Figure 10 Confidential and personal data flows

Scenario 13: Sandra

As-is scenario 13.1: Sandra


	<p>Actor: Sandra Sandra is 39 years old, working as an accountant, she is active on social media, owns a smartphone and several other IT devices.</p> <p>Role in the Cloud ecosystem: Individual Employee and end user of cloud services (cloud user; individual end user)</p> <p>Computer experience: She is skilled</p>	<p>Problem Scenario told by Sandra: Sandra, an individual end user, accesses business productivity cloud applications provided by her employer enterprise ecosystem. She uses a single device for personal and business usages, accessing cloud-services for personal and business purposes from the same device. As a result, her device is at the intersection of policy enforcement of different IT domains with which she interacts via cloud services, thus raising new accountability challenges. To the extent that her personal data may be replicated or synchronized with cloud data storage services, the accountability issues span across devices and cloud services. She is concerned that her user profile information and personal data may be subject to cloud service policies signed by her employer as well as by her for personal usage. She currently has no way of checking whether any personal data is subject to employer scrutiny due to business cloud policies signed by her employer.</p>
---	--	--

To-be scenario 13.1.1


	<p>Scenario 13.1.1a: Sandra (as individual end user) will be able to comply with specific rights and obligations with respect to treatment of data (data governance), although she has little idea what her obligations are. Although the employer for any business misconduct could hold the individual end user responsible, as owner of the device, it is possible that Sandra's employer is a data controller of her employer's information, jointly with her employer (the law is completely unclear on this) and if so will owe obligations to the regulator directly. Under the law of confidence she may well owe obligations directly to business customers (as different from individual data subjects, under data protection law data subjects are in most countries individuals only).</p>
	<p>Scenario 13.1.1b: Sandra (as individual end user) will be able to set data policies to be associated with specific personal data as transferred to the cloud service.</p>
	<p>Scenario 13.1.1c: Sandra (as individual end user and data subject) will be able to access policy violation information about the cloud services she is using (for her own personal data). In particular, she will have access to real-time assessment (either quantitative or qualitative) if data policies have been violated by cloud services.</p>
	<p>Scenario 13.1.1d: Sandra (as individual end user) will be aware whether or not she is complying with business corporate guidelines on cloud service usage. She will be notified whether or not data policies have been fulfilled throughout cloud service chains.</p>
	<p>Scenario 13.1.1e: Sandra (as individual end user and data subject) will have (either quantitative or qualitative) information about policy violation (or compliance) from the cloud service she is using (for her own personal data).</p>
	<p>Scenario 13.1.1f: Sandra (as individual end user) will be able to report to the service provider (and if necessary directly to data protection authorities) any policy violation she is experiencing.</p>
	<p>Scenario 13.1.1g: Sandra (as individual end user) will be notified about any policy violation occurring throughout the cloud supply chain.</p>

Scenario 14: Paul

As-is scenario 14.1: Paul

	<p>Actor: Paul is the Chief Privacy Officer (CPO) of a SME that is moving most of its services to the Cloud. He has been constantly supporting security and privacy programs to enhance vulnerability awareness of employees. He is also responsible for compliance of IT systems with respect to relevant legislations.</p> <p>Role in the Cloud ecosystem: IT Company's Chief Privacy Officer (CPO); Business consumer (Cloud service user)</p> <p>Computer experience: Expert on IT laws</p>	<p>Problem Scenario told by Paul: In order to comply with current legislation on data protection and to secure business data, the CPO is currently constraining the use of cloud services, within the employer enterprise ecosystem and its business productivity cloud applications, by employees. The main concerns are due to the fact that employees (Individual end users) are increasingly going to be using a single device for personal and business use, accessing cloud-services for personal and business purposes from the same device. Accountability issues arise for enterprise data as it is cached or replicated across a potential range of end user devices that may be increasingly end user owned devices. A further concern is that end users may subscribe to and use unknown cloud services (e.g. for backup or synchronisation) without his permission or even knowledge.</p>
---	--	---

To-be scenario 14.1.1


	<p>Scenario 14.1.1a: Paul (as cloud business user on behalf of his employer) will be able to provide evidence of compliance with respect to relevant legislative regimes, if required by Auditors. Moreover, the employer is directly responsible to both data subjects as well as regulatory authorities for any misconduct with respect to data governance. If data governance is proved to comply with relevant regulatory regimes, the risk of non-compliance can be mitigated and managed throughout accountability chains of cloud service provision.</p>
---	--

D:B-3.1 Use Case Descriptions


<p>Scenario 14.1.1b: Paul (as cloud business user on behalf of his employer) will be able to set data policies for the cloud services adopted by his IT Company. These data policies will apply to all devices used to access such cloud services. Auditing these devices may become necessary to support the enforcement of the data policies. They will also constrain the use of cloud services by company employees.</p>
<p>Scenario 14.1.1c: Paul (as cloud business user on behalf of his employer) will be able to access policy violation information about the cloud services used by his IT Company. In particular, he will have access to real-time assessment (either quantitative or qualitative) if data policies have been violated by cloud services.</p>
<p>Scenario 14.1.1d: Paul (as cloud business user on behalf of his employer) will be notified about any policy violation occurring throughout the cloud supply chain.</p>
<p>Scenario 14.1.1e: Paul (as cloud business user on behalf of his employer) will be able to notify relevant subjects (e.g. customers as well as employees) about any incident occurring throughout the cloud supply chain. Notifications can be automatically generated depending of the required data policies and service level agreements.</p>

Scenario 15: Roger

As-Is Scenario 15.1:


	<p>Actor: Roger is the Chief Technology Officer (CTO) of a Cloud Service Provider. He is responsible for the operational management of cloud services and their compliance with relative Data Protection legislations.</p> <p>Role in the Cloud ecosystem: Cloud Service Provider</p> <p>Computer experience: Security expert; Software Engineer</p>	<p>Problem Scenario told by Roger: Roger is aware that in order to enhance service competitiveness, cloud services would need to listen to customer needs. He knows that security and privacy are among the main concerns of cloud users (due to the increasing threats to personal and confidential data). Therefore, on the one hand, he needs to maintain good customer relationships. On the other hand, he needs to make sure that cloud services rely on trustworthy business partners (that is, other cloud service providers).</p>
---	---	---

To-Be Scenario 15.1.1


	<p>Scenario 15.1.1a: Roger (as CTO of cloud service provider) will be able to access policy compliance information about alternative cloud infrastructure providers. This information will be used either to select which services to rely on or to provide different services. It will be also useful to conduct internal auditing processes as well as to provide information for external auditing.</p> <p>Scenario 15.1.1b: Roger (as CTO of cloud service provider) will be able to draft different contracts with cloud users as well as other cloud providers depending on the service levels required and risk/trustworthiness profiles of involved parties.</p> <p>Scenario 15.1.1c: Roger (as CTO of cloud service provider) will be able to enforce data policies throughout cloud supply chains as requested by cloud users.</p> <p>Scenario 15.1.1d: Roger (as CTO of cloud service provider) will be able to notify cloud users about any incident occurring throughout cloud supply chains.</p> <p>Scenario 15.1.1e: Roger (as CTO of cloud service provider) will be able to assess the risk associated (in terms of policy violations) with alternative cloud providers while considering transferring data to and relying on them. His assessment will take into account trustworthiness information and risk profiles of alternative service providers.</p> <p>Scenario 15.1.1f: Roger actively searches for the needs and concerns of cloud users (responsiveness) and decides what actions he can perform and what not.</p>
---	--

Scenario 16: Michael

As-is scenario 16.1: Michael


	<p>Actor: Michael</p> <p>Role in the Cloud ecosystem: Cloud Auditor</p> <p>Computer experience: Knowledgeable; Expert in IT laws</p>	<p>Problem Scenario told by Michael: Michael is responsible for assessing how cloud service providers comply with relevant Data Protection legislations. Currently, he needs to inspect practices and collect evidence throughout cloud supply chains. The increasing number of service providers as well as their exposures to threats makes his daily job very challenging. Moreover, due to limited resources, he is aware that it is unfeasible to exhaustively check all parties throughout cloud supply chains. He is concerned that despite any effort he might miss and misjudge any critical information and therefore expose cloud users to potential threats.</p>
---	---	---

To-be scenario 16.1.1


	<p>Scenario 16.1.1a: Michael (as cloud auditor) will be able to assess regulatory and data policy compliances of cloud service providers by accessing relevant operational evidence collected by service providers. Operational evidence of cloud services will also include relevant information about business partners (i.e. other cloud services) in the cloud supply chain as well as how providers addressed emerging issues and user complaints.</p>	
	<p>Scenario 16.1.1b: Michael (as cloud auditor) will be able to certify, with an increased level of confidence, “no evidence found of non-compliance” with respect to current data protection legislations (and derived obligations).</p>	

Scenario 17: John

As-is scenario 17.1: John

	<p>Actor: John</p> <p>Role in the Cloud ecosystem: Regulator (Data Protection Authority)</p> <p>Computer experience: Expert in data protection, privacy and IT laws</p>	<p>Problem Scenario told by Michael: John is responsible for addressing the application of data protection legislations by cloud service providers and cloud service users (acting as data controllers or data processors) in the interest of individual data subjects. He will issue notice or penalties for any data protection breach. He is currently struggling due to lengthily evidence collections for reported data breaches. It is very difficult to dispute evidence of governance malpractices¹⁹.</p>
---	--	---

To-be scenario 17.1.1

	<p>Scenario 17.1.1a: John (working for the national Data Protection Authority) will be able to investigate reported data protection infringements by reviewing operational evidence of parties involved in reported incidents.</p>	
	<p>Scenario 17.1.1b: John (working for the national Data Protection Authority), based on the collected operational evidence, will be able to initiate the processes which might lead to sanctions to cloud service providers depending on the severity of reported data protection infringements.</p>	

¹⁹ Note that issues of law relating to evidence collection and use are very different in every country, and outside project scope.

Healthcare IT domain

As-Is Scenarios for (2) a healthcare IT domain via e-government type cloud services available to citizens. From a cloud service perspective, we will assume a single IaaS provider that operates both the enterprise employee cloud application services and the government health care cloud service, in order that we can analyse accountability modelling and tracking at the intersection of the end user, IaaS provider, enterprise, and healthcare service operator. We will further assume that at least one of the cloud service providers relies on a cloud service provided by yet another cloud service provider. Finally, we will analyse how to ensure accountability of the enforcement of confidentiality and integrity guarantees over employee personal data, personal healthcare data and enterprise business data across the stakeholder interfaces. Figure 11 highlights the healthcare data flows.

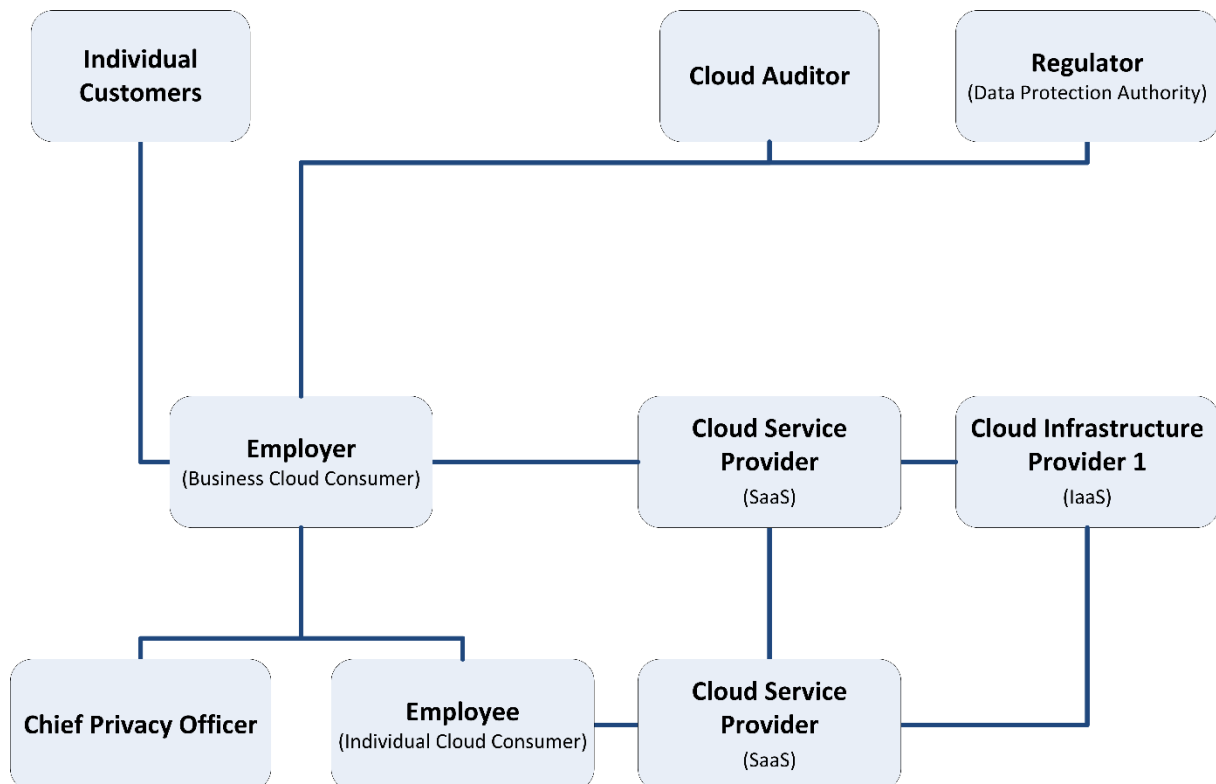




Figure 11 Business and personal data flows

Scenario 18: Sandra

As-is Scenario 18.1: Sandra


	<p>Actor: Sandra Sandra is 39 years old, working as an accountant, she is active on social media, owns a smartphone and several other IT devices. She is daughter to Kim (72 years) who is registered in the Ageing Well program.</p> <p>Role in the Cloud ecosystem: Individual Employee and end user (Cloud service user)</p> <p>Computer experience: She is skilled</p>	<p>Problem Scenario told by Sandra: Sandra uses a single device for personal and business usages, accessing cloud-services for personal and business purposes from the same device. She is using her device to monitor and access information about a healthcare service arranged by her father. As individual end user, she accesses her personal data as well as her father data provided (according to specified data restriction) by a Cloud Service Provider in the Healthcare domain. She is concerned how personal data (related to such healthcare service) may be aggregated to other healthcare data held by her Employer that stores HR information (e.g. healthcare insurance, private medical plan) in other cloud healthcare services.</p>
---	---	---

To-be scenario 18.1.1


	<p>Scenario 18.1.1a: The individual end user will have specific assurance about how personal data is treated by a Cloud Service Provider in the Healthcare domain.</p>
	<p>Scenario 18.1.1b: Healthcare IT domain via e-government type cloud services available to citizens. The (Healthcare) Cloud Service Provider will be held accountable by auditors and end users for handling of personal data.</p>

Scenario 19: Linda

As-is scenario 19.1: Linda


	<p>Actor: Linda</p>	<p>Problem Scenario told by Linda: The main concern is to maintain and satisfy the SLA (Service Level Agreement) with the cloud business user by storing and maintain updated information about data subjects (e.g. company employees)</p>
	<p>Role in the Cloud ecosystem: HR's Cloud Service Provider (SaaS)</p> <p>It provides healthcare related services to the cloud business user's Human Resources</p> <p>Computer experience: Security Expertise</p>	

To-be scenario 19.1.1


	<p>Scenario 19.1.1a: She will be able to enforce data policies throughout cloud supply chains as requested by cloud users.</p>
--	---

Scenario 20: Peter

As-is scenario 20.1: Peter

	<p>Actor: Peter Peter works for the Healthcare Cloud Service signed by Sandra's father (Kim).</p>	<p>Problem Scenario told by Peter: The main activities are concerned with passing relevant information to other service providers in order to address any emerging needs related to service provisions. Peter is working according to specified service level agreements. However, he might not be aware of any conflicting requirements between cloud services due to data manipulation and aggregation.</p>
	<p>Role in the Cloud ecosystem: Cloud Service Provider – Healthcare IT domain via e-government type cloud services available to citizens.</p> <p>Computer experience: He is skilled – knowledgeable about Security and Privacy</p>	

To-be scenario 20.1.1

	<p>Scenario 20.1.1a: Healthcare IT domain via e-government type cloud services available to citizens. The (Healthcare) Cloud Service Provider will be held accountable by auditors and end users for handling of Personally Identifiable Information (PII).</p>
---	--