
D:D-7.2: Final system and use case prototype

Deliverable Number	D47.2
Work Package	WP 47
Version	1.0
Deliverable Lead Organisation	ATC
Dissemination Level	PU
Contractual Date of Delivery (release)	30/11/2015
Date of Delivery	31/03/2016

Editor

Vasilis Tountopoulos (ATC)

Contributors

Giorgos Giotis (ATC), Richard Brown (ATC), Anderson Santana de Oliveira (SAP), Thomas Ruebsamen (HFU), Rehab Alnemr (HPE), Massimo Felici (HPE), Michela D' Errico (HPE), Jean-Claude Royer (EMN), Christian Frøystad (SINTEF), Philip Ruf (HFU), Christoph Reich (HFU)

Reviewers

Tobias Pulls (KaU), Melek Onen (Eurecom)

Executive Summary

A4Cloud advances research on accountability, which is critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. The research being conducted in the project aims to support establishing trust in cloud computing by devising methods and tools, through which cloud stakeholders can be made accountable for how they manage personal, sensitive and confidential information in the cloud. Such methods and tools delivered by the A4Cloud project combine risk analysis, policy enforcement, monitoring and compliance auditing, contributing to the effective governance of cloud activities, providing transparency and assisting policy enforcement in an inter-disciplinary co-design approach, which implements accountability from a technical, legal, regulatory and socio-economic perspective.

This deliverable aims to present the instantiation of the results from the A4Cloud project in the real life example, servicing the data protection and privacy requirements of the wearables business domain. More specifically, the document summarises the adoption of the lifecycle for accountability from the perspective of all the business actors involved in the wearables use case, who are embodied a certain cloud and data protection role in the collection and processing of personal data. To this end, the A4Cloud use case prototype exploits the accountability mechanisms and support services and implements accountability across the cloud service supply chain of the wearables use case, from a preventive (mitigating risk), detective (monitoring and identifying risk and policy violation) and corrective (managing incidents and providing redress) way.

From a technical point of view, this final version of the A4Cloud prototype describes how the A4Cloud tools enable cloud providers to define, enforce and monitor policy rules in response to compliance with established regulations and business policies. Subsequently, through the appropriate implementation of the respective measures, the cloud providers can provide design time and runtime verification of their alignment to data protection concerns. Furthermore, the final instantiated prototype provides tool support for cloud customers in making informed choices on how selected cloud providers would protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices. Finally, this deliverable showcases how the cloud subjects are empowered with data subject control tools to take control over how their data is handled in the cloud.

The wearables use case has been developed with the scope to demonstrate the instantiation of the accountability framework, the cloud accountability reference architecture and the respective tools developed by the A4Cloud project in a real life example. The use case constitutes a realistic and topical scenario, in which the involved business actors have to take the appropriate actions to ensure that the occurred collection and processing of customers' personal data from wearable devices are handled responsibly, based on the established regulations and the declared organisational policies, which address specific security and privacy requirements.

The presentation of the final use case prototype puts emphasis on the demonstration of the prototype versions of the accountability tools, as they have been developed within the A4Cloud project, and elaborates on the implementation of accountability in regards to the accountability support services. The deliverable succeeds in presenting an accountability based analysis of the wearables use case and providing the implementation of an integrated proof of concept demonstrator for the A4Cloud prototype. This use case prototype includes the integration of the A4Cloud tools and their customisation into the wearables use case, while it demonstrates the support for accountability from the perspective of the different roles, namely the cloud provider, the cloud customer, the data subject and the cloud auditor. Through the five demonstration scenarios presented in this document, we have manage to address the view of all these roles in the implementation of accountability.

Finally, the document offers guidance on how the developers of use case applications in the cloud can utilise the whole set of the A4Cloud toolkit and integrate the respective tools and artefacts into their implementation environment to address the privacy and data protection requirements of the actors involved in their project. Through these guidelines, the developers will understand how to instantiate the cloud accountability reference architecture and integrate the respective A4Cloud tools for the implementation of accountability mechanisms in their application.

Table of Contents

Executive Summary	2
1 Problem Definition	7
1.1 Introduction	7
1.2 The Scope of the Final Prototype	7
1.3 Structure.....	8
1.4 Glossary of Acronyms / Abbreviations	8
2 Guidance on the adoption of the Accountability Framework	10
2.1 Defining the cloud service supply chain.....	10
2.2 Adopting the lifecycle for accountability	11
2.2.1 Cloud customer being a data controller	11
2.2.2 Cloud service provider being a data processor.....	12
2.2.3 Client as a data subject	13
2.3 Implementation of the accountability support services	13
2.3.1 Policy definition and validation	13
2.3.2 Policy management and enforcement.....	15
2.3.3 Monitoring and environment state collection	16
2.3.4 Collection and management of evidence	17
2.3.5 Incident Management.....	17
2.3.6 Notification.....	18
2.3.7 Remediation	19
2.3.8 Validation.....	20
2.4 Summary of the tools usage	22
3 Updates on the specifications for the wearables use case	27
3.1 Overview of the wearable service	27
3.2 The accountability-based analysis of the Wearable Service	28
3.2.1 The accountability lifecycle for the Wearable Co	28
3.2.2 The accountability lifecycle for Kardio-Mon.....	30
3.2.3 The accountability lifecycle for Map-on-Web	32
3.2.4 The accountability lifecycle for DataSpacer	32
3.2.5 The accountability lifecycle for the Wearable Co Customer	33
4 Implementation of the final prototype	34
4.1 Instantiating the Cloud Accountability Reference Architecture for the wearables use case... 34	
4.1.1 The perspective of the Wearable Co.....	34
4.1.2 The perspective of Kardio-Mon	35
4.1.3 The perspective of Map-on-Web.....	38
4.1.4 The perspective of DataSpacer.....	40
4.1.5 The perspective of the Wearable Co Customer	42

4.2	The physical deployment of the wearables use case components	42
4.3	The use of A4Cloud tools in the implementation of the wearables use case	44
4.3.1	Policy Definition and Validation	45
4.3.2	Policy Management and Enforcement	46
4.3.3	Monitoring and Environment State Collection	46
4.3.4	Collection and Management of Evidence.....	47
4.3.5	Incident Management.....	47
4.3.6	Notification.....	48
4.3.7	Remediation	49
4.3.8	Validation.....	49
4.4	Concluding the implementation of the use case prototype	50
5	Demonstration of the wearables use case	51
5.1	Introducing the demonstration scenario.....	51
5.1.1	The history of the scenario	51
5.1.2	The demonstration scenarios	52
5.2	Demo Scenario 1: Selection of the cloud service supply chain	56
5.2.1	Scope	56
5.2.2	Actors Involved.....	57
5.2.3	Description of the demo scenario.....	57
5.2.4	Addressing the Accountability Framework	57
5.2.5	Prerequisites.....	57
5.2.6	The scenario steps	57
5.2.7	Outcome	64
5.3	Demo Scenario 2: Implementation of policies	64
5.3.1	Scope	64
5.3.2	Actors Involved.....	65
5.3.3	Description of the demo scenario.....	65
5.3.4	Addressing the Accountability Framework	65
5.3.5	Prerequisites.....	65
5.3.6	The scenario steps	65
5.3.7	Outcome	72
5.4	Demo Scenario 3: Incident Management.....	72
5.4.1	Scope	72
5.4.2	Actors Involved.....	72
5.4.3	Description of the demo scenario.....	72
5.4.4	Addressing the Accountability Framework	73
5.4.5	Prerequisites.....	74
5.4.6	Scenario Steps	74
5.4.7	Outcome	76

5.5	Demo Scenario 4: Monitoring and Audit	77
5.5.1	Scope	77
5.5.2	Actors Involved	77
5.5.3	Description of the demo scenario	77
5.5.4	Addressing the Accountability Framework	78
5.5.5	Prerequisites	78
5.5.6	Scenario Steps	78
5.5.7	Outcome	81
5.6	Demo Scenario 5: Data Subject Controls	81
5.6.1	Scope	81
5.6.2	Actors Involved	81
5.6.3	Description of the demo scenario	81
5.6.4	Addressing the Accountability Framework	81
5.6.5	Prerequisites	82
5.6.6	The scenario steps	82
5.6.7	Outcome	84
6	Supporting the Provision of the Account	85
6.1	Evidence-Based Accountability	85
6.2	Assurance of Cloud Supply Chain	85
6.3	Structuring the Provision of the Account	86
6.3.1	Evidence of Cloud Controls	87
6.3.2	Linking Controls to Supporting Evidence	88
6.3.3	Roles in Providing Assurance	89
6.3.4	Evidence Access	89
6.4	Assurance for the Demonstrator Scenario	90
6.4.1	An Assurance Example: Implementing SLAs	91
6.4.2	Demonstrator Access Configuration	92
6.5	Security and Privacy Assurance Case Environment	92
7	Conclusions	95
8	References	96
9	Appendices	97
9.1	Specifications of the wearable use case	97
9.1.1	The list of personal data	97
9.1.2	The machine readable accountability policy	97
9.1.3	Machine readable policy for DTMT configuration	111
9.2	The operation of the Web-based Wearable application	113
9.2.1	The operations of the Wearable Co customer	113
9.2.2	The operations of the Wearable Co Employee	119
9.3	Examples of evidence records stored in AAS	121

9.3.1	Evidence Record Generated from A-PPLE Logs	121
9.3.2	Evidence Record Generated from OpenStack Nova Service	122

1 Problem Definition

1.1 Introduction

Cloud data governance is a fundamental problem in current Internet-based applications, which sets barriers to the wider adoption of cloud technologies for a variety of domain specific applications. The problem of effective governance and control of personal data requires from cloud providers and customers to be accountable to the owners of personal data for their data handling procedures. The A4Cloud project conducts advanced research on accountability, which is the prerequisite for adequate governance and transparency, by delivering the accountability framework and a set of tools to address the requirements of various stakeholders involved in the cloud service delivery chain.

More specifically, the A4Cloud project has developed a conceptual model for accountability [1], which defines accountability attributes, practices and mechanisms and how they relate to each other. The accountability mechanisms incorporate legal, regulatory, socio-economic and technical approaches, which are integrated into a framework to support an accountability-based cloud approach to cloud data governance and are functionally classified into preventive, detective and corrective mechanisms.

The project delivers the A4Cloud toolkit, as an Appendix to [3], which aims to support the implementation of these mechanisms. The tools comprising this toolkit are designed considering the existing gaps in accountability practices, thus, they aim to implement those functions of the accountability mechanisms, for which little or no support was found to exist out there to complement current privacy and security mechanisms. The definition and the design principles of the toolkit are based on the fact that each A4Cloud tool addresses different elements of accountability, and may operate over different time scales, while interacting with data at different stages of data life cycle. Thus, the tools implementing preventive mechanisms investigate the potential risks in cloud data stewardship in order to form policies and decide on relevant mechanisms that should be followed. The tools implementing detective mechanisms put in place detection and traceability measures to monitor misbehaviours, such as policy violations, in the normal operation of cloud processes. Finally, the tools implementing corrective mechanisms provide notification and remediation, as a response to detected anomalies of the cloud service chains.

Following the initial use case prototyping of the A4Cloud project in Deliverable D47.1 [2], this deliverable reports on the final version of the A4Cloud use case prototype for the wearables use case. The development activities have followed the progress of the activities for the specification of the cloud accountability reference architecture in [3] and as such the use case development is presented from the perspective of the implementation of the lifecycle for accountability.

1.2 The Scope of the Final Prototype

In this final prototype, we update the specifications of the wearables use case and we analyse the roadmap to demonstrate the accountability concepts through a prototype implementation of the Wearable Service. The latter is a cloud service, which is designed and hosted in the cloud, so that the involved cloud providers and the cloud customer are accountable for their data handling procedures in compliance with the established regulations and business organisational processes brought into the market by the relevant actors.

The final use case prototype covers the whole set of the A4Cloud toolkit and, thus, it integrates the A4Cloud tools and artefacts from an end-to-end approach, in order to demonstrate how accountability can be implemented along the supply chain of the actors involved in the wearables use case for addressing the privacy and data protection requirements of the end users disclosing their personal data in the cloud environment. Thus, through this document, we implement the wearables use case and illustrate how the tools comprising the A4Cloud toolkit, introduced in [3], are interfacing with each other and with the components of the wearables use case and working together across a real life cloud service supply chain.

The presentation of the final use case prototype puts emphasis on the demonstration of the prototype versions of the accountability tools, as they have been developed within the A4Cloud project, and elaborates on the implementation of accountability in regards to the accountability support services. Subsequently, the demonstration should showcase how the A4Cloud tools can be adopted by the actors of the wearables use case and work for each of them, based on their cloud and data protection role.

1.3 Structure

In order to address the envisaged work for the final prototype, this document is structured as follows:

- Section 2 provides a set of guidelines for the developers of use case applications in the cloud on how to use the A4Cloud tools in the context of a reference cloud environment.
- Section 3 updates on the specifications of the wearables use case since Deliverable D47.1 and presents the adoption of the lifecycle for accountability for the different actors of this use case.
- Section 4 goes deeper into the details of the technical implementation of the final use case prototype. It presents the final physical deployment and the implementation of the guidelines for the specific wearables use case.
- Section 5 introduces the scenarios used to demonstrate how accountability is implemented for the business actors of the wearables use case.
- Section 6 goes beyond the implementation of the wearables use case and aims to point out the role of evidence in the provision of the account and how the resulting work in the A4Cloud use case prototyping can support assurance and trustworthiness for the involved business cloud actors.
- Finally, Section 0 summarises the contents of this deliverable and refers to the lessons learnt.

1.4 Glossary of Acronyms / Abbreviations

Acronym / Abbreviation	Description
AAL	Abstract Accountability Language
AAS	Audit Agent System
AccLab	Accountability Lab
A-PPL	Accountable Primelife Policy Language
A-PPLE	Accountable Primelife Policy Engine
CARA	Cloud Accountability Reference Architecture
COAT	Cloud Offerings Advisory Tool
CSIRT	Computer security incident response team
CSP	Cloud Service Provider
CTP	CloudTrust Protocol
DPIAT	Data Protection Impact Assessment Tool
DPPT	Data Protection Policies Tool
DT	Data Track
DTMT	Data Transfer Monitoring Tool
EEA	European Economic Area
IaaS	Infrastructure-as-a-Service
IMT	Incident Management Tool
PLA	Privacy Level Agreement
PO	Privacy Officer
RRT	Remediation and Redress Tool
SaaS	Software-as-a-Service

Acronym / Abbreviation	Description
SLA	Service Level Agreement
SME	Small-Medium Enterprise
TL	Transparency Log
UI	User Interface
VM	Virtual Machine

2 Guidance on the adoption of the Accountability Framework

This section provides a set of guidelines for the developers of use case applications in the cloud on how to use the A4Cloud tools. More specifically, it presents the solution offered by the Cloud Accountability Framework in order to develop business application use cases through a step-by-step approach. The evolution of the steps addresses the accountability lifecycle and the relevant accountability support services to implement the functional elements of this cycle.

It must be noted that by referring to developers of the use case applications we do not restrict the guidelines to those implementing the software solution, but we are trying to extend as much as possible to other actors being involved in the definition, design, implementation and operational deployment of the use case application.

2.1 Defining the cloud service supply chain

For the analysis in this section, we are inspired by the wearables use case, which is exploited in A4Cloud to demonstrate the accountability aspects between the business actors involved in it. To this end, we present the guidelines for use case developers, based on the analysis performed in WP42 and the final version of the Cloud Accountability Reference Architecture in D42.4 and the A4Cloud tools documentation.

For these guidelines, we adopt the relationships of the business actors shown in Figure 1. In this figure, we define a cloud customer, being a data controller without any ICT skills or IT infrastructure, which set ups a cloud business, based on the cloud service offered by the primary cloud service provider (this is a data processor in this case). The cloud customer operates a business to their clients, who are data subjects by providing their personal data to the cloud service. Apart from the primary cloud service provider (CSP), the cloud environment consists of the cloud IaaS and SaaS providers, who complement the primary CSP in offering their cloud service. The cloud business reference environment is completed with the external cloud auditor, who is responsible for performing external audits to the CSPs.

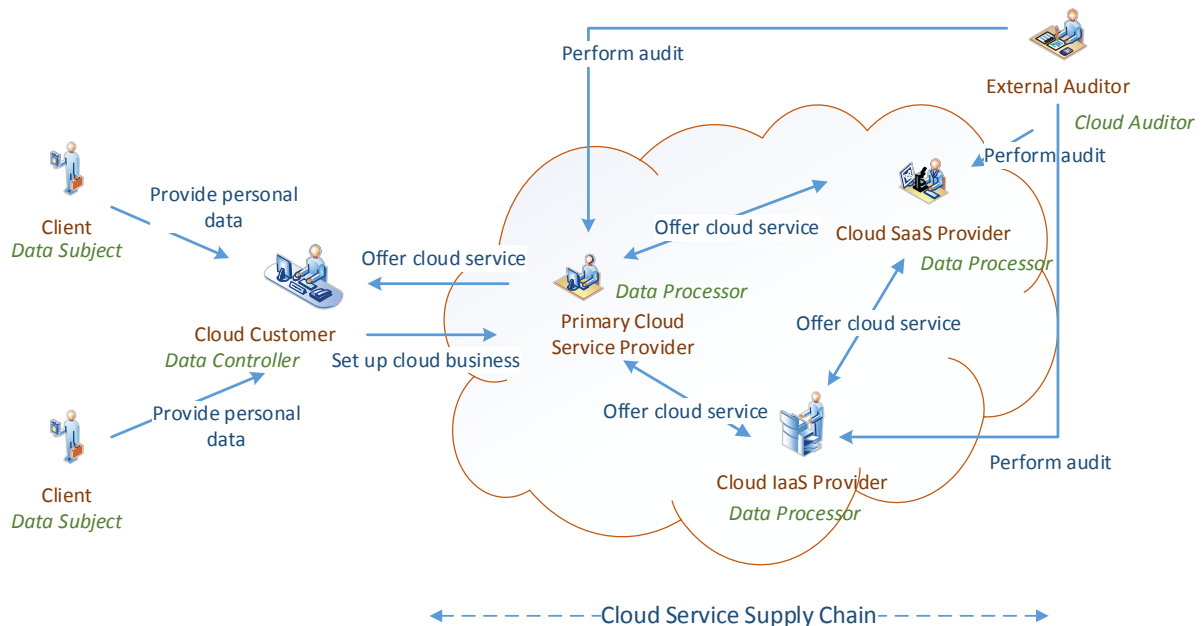


Figure 1: The cloud business reference environment for the guidelines

Based on the reference environment, the guidelines in this section drive the use case developers in implementing the appropriate accountability aspects for the protecting of the personal data involved in the execution of the business scenario (the clients' personal data). The presentation of the guidelines is following the accountability support services. As such, the different business actors are attributed a cloud and a data protection role, which is exploited to determine the processes that the actors should execute, with the aid of the A4Cloud tools.

2.2 Adopting the lifecycle for accountability

For the cloud business reference environment, each identified actor is to adopt the lifecycle for accountability, which is presented in Figure 2. This means that all the identified actors should go through the lifecycle phases and demonstrate how they follow the respective functional elements, by adopting accountability practices and implementing respective accountability mechanisms.

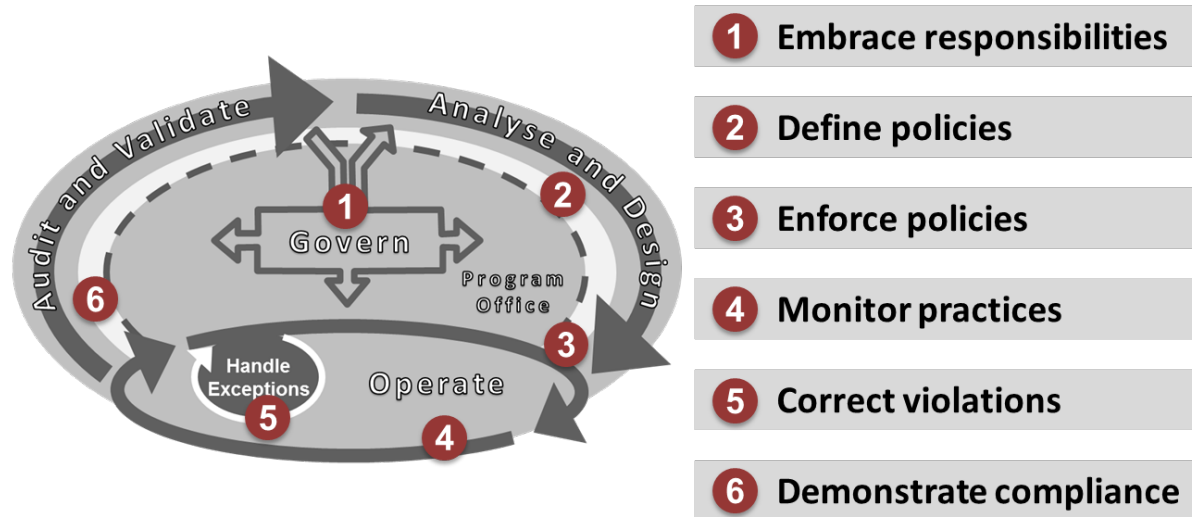


Figure 2: The phases of the Accountability Lifecycle

The remaining of this section is devoted to the description on how each business actor, being attributed a specific cloud and data protection role is running the lifecycle phases for accountability. Due to the fact that all the involved cloud providers are data processors in our example of Figure 1, the presentation of the primary CSP, the cloud SaaS provider and the cloud IaaS provider is done in the same section, emphasising on the different sub-cases.

2.2.1 Cloud customer being a data controller

This actor is responsible for driving the data controlling processes on how the personal data collected from individuals should be handled. This actor runs the following phases:

- **Embrace responsibilities:** in this phase, the cloud customer documents the obligations for running the cloud business, according to legal and social norms. To this end, in this phase, the cloud customer accepts the responsibility for being aware of the risks arising from their decision and the potential implications from the exposure of these risks.
- **Define policies:** in this phase, the cloud customer expresses their functional, security and privacy requirements to determine on which cloud service supply chain is the most appropriate one to work with. The analysis in this phase includes the selection of the primary CSP and their third party collaborators, namely the SaaS and IaaS CSPs, the performance of a data protection impact assessment, detailing the risks that this actor should run in getting in business with this supply chain, and the identification of security controls, which would allow the cloud customer to implement a risk treatment plan. The policy definition phase, also, refers to the negotiation and agreement between the cloud customer and the primary CSP on which accountability policies must be enforced to address the cloud customer's requirements, subject to the capabilities of the selected cloud service supply chain.
- **Enforce Policies:** in this phase, the cloud customer requests for an account from the primary CSP for the enforcement of the agreed policies along the cloud service supply chain.
- **Monitor Practices:** in this phase, the cloud customer must be able to assess the normal operations of the service supply chain and respond to any requests arising from the clients.

- **Correct Violations:** in this phase, the cloud customer reacts in case that an incident is notified from the primary CSP or reported from the clients, referring to an abnormal situation happened with the personal data of the clients or the environment hosting this data.
- **Demonstrate Compliance:** in this phase, the cloud customer shall be able to allow the CSPs or the cloud auditor, to request for an account for the validation of the cloud customer's data handling practices through audits.

2.2.2 Cloud service provider being a data processor

In the given reference environment of Figure 1, the cloud providers being displayed there are responsible for offering a specific type of cloud service to their customers, either being the cloud customer if this section refers to the primary CSP, or another cloud provider if it refers to the cloud SaaS or IaaS provider. The actors run the following phases:

- **Embrace responsibilities:** in this phase, the cloud accepts the responsibility for being transparent in the delivery of the cloud service to their customers. The involvement of a cloud provider in this phase ranges from the time, in which this actor conceptualises the design of the cloud service, up to the time, in which this actor accepts the responsibility for advertising their functional, security and privacy capabilities towards establishing new contracts with potential customers (either cloud customers, if we are talking about the primary CSP, or cloud providers).
- **Define Policies:** in this phase, a CSP is involved to select the collaborating cloud providers, through a data protection impact assessment process, and run the appropriate mechanisms in order to define the policies for establishing a business relation or contract with another actor. For example, the role of the primary CSP in this phase can be in the case that the cloud customer requests for an accountability policy to establish an agreement for operating the cloud service. In another example, the role of a CSP in this phase lays on the policy checking and matching activities, in which one CSP wants to validate that the contract offered by a second CSP is aligned to both the data protection preferences of the first CSP and the functional, security and privacy capabilities of the second CSP.
- **Enforce Policies:** in this phase, the role of the CSP is to implement the mechanisms for the enforcement of the policies and provide an account to the collaborating CSPs or cloud customers (in case of the primary CSP) for the implementation of these enforcement mechanisms. Depending on the position of the CSP in the cloud service supply chain, the involvement of the CSP in the enforcement of the policies may vary. For example, the primary CSP is responsible for the enforcement of all the rules in the policies agreed with the cloud customer, thus the primary CSP provides an account to the cloud customer for the enforcement of the policies, either they are enforced in their territory or in the territory of another CSP.
- **Monitor Practices:** in this phase, the CSP monitors the execution of their cloud service and collects and stores information about this operation. Through the deployment of the appropriate tools, the CSP collects and analyses logs from the cloud environment and compiles them into searchable evidence on how the CSP undertakes the claimed data handling procedures. The respective evidence may refer to both the proper operation of the cloud service and any potential incidents that may raise an abnormal behaviour of the CSP environment. Depending on the type of the CSP, the monitoring processes may span across different layers of the cloud protocol stack. For example, an IaaS CSP monitors the implementation of controls on the network layer (i.e. logging information about transfer of data across different networks), while a SaaS CSP monitors the implementation of controls on the service layer, regarding the enforcement of data access rules.
- **Correct Violations:** in this phase, the CSP analyses the collected monitoring logs and evidence in order to detect incidents in the cloud environment. These incidents may refer to potential security breaches or policy violations occurring the territory of the CSP or outside of it, which are perceived by the CSP or reported to them through the collaborating CSPs. The role of the CSP in this case is also on issuing notifications about these incidents and running the internal processes for responding to these incidents, including the support for the implementation of remediation actions
- **Demonstrate Compliance:** in this phase, the CSP is responsible for providing an account to the other CSPs (or the cloud customer in case of the primary CSP) or the auditor and the supervisory

authorities about their data handling procedures, considering that they have already validated the respective procedures of their third party CSPs.

2.2.3 Client as a data subject

In the given reference environment of Figure 1, this actor is the end user, who is consuming the accountability offering of the cloud customer (as the provider of the cloud business to this client) within the environment being set up by the CSPs. This actor does not demonstrate compliance with the accountability practices to any other actor and, as such, the client is only participating in the phases of the lifecycle for accountability, when interacting with the cloud customer and / or the primary CSP, as follows:

- **Embrace responsibilities:** in this phase, the client accepts the risks stemming from their decision to access the cloud service and give their consent to the cloud customer and the primary CSP to collect and process their personal data, according to the rules of the agreed policies.
- **Define policies:** in this phase, the client may submit to the cloud customer their preferences for certain data protection options, like maximum data retention time, allowable geographical locations for data storage, etc.
- **Enforce policies:** in this phase, the client gives consent for the collection of their personal data and processing it in the cloud.
- **Correct violations:** in this phase, the client exercises their right to be informed of any incidents happening in the cloud chain that should be notified to them, because of the potential impact of these incidents on their privacy. In this phase, the client can, also, take the provided measures to respond to these incidents, according to the established regulation and the agreed policy.
- **Demonstrate compliance:** in this phase, the client may contact the Supervisory Authority and ask for an audit on the cloud customer or the primary CSP (and their third parties), as a result of responding to a notification. Also, the client is able to validate the data handling practices of the cloud customer and the cloud environment and assess whether the adopted mechanisms for providers for the management of data disclosure are operated in accordance to the accepted policies.

2.3 Implementation of the accountability support services

Following the adoption of the phases of the lifecycle for accountability from the perspective of the business actors involved in the reference cloud environment of Figure 1, in this section, we present guidelines for the implementation of the accountability support services through the use of the A4Cloud tools. The guidelines explain the actions that the business actors of Figure 1 should undertake along the implementation of the accountability support services, making specific references to the use of the tools in each service. In order to set the boundaries of the guidelines, we assume that the reference cloud environment in Figure 1 has been set up and, thus, the guidelines refer to the activities being evolved at the time that the cloud customer decide to run a cloud business.

2.3.1 Policy definition and validation

The activities in this service involve the establishing of bilateral agreements between the CSPs and with the cloud customer in order to run the cloud business. The reference cloud environment is dynamically built by allowing the primary CSP to select the third party CSP, which act complementary to this actor in order to operate the cloud service. The selection process involves the CSPs to advertise their functional, security and privacy requirements through the Service Level Agreements (SLAs) they offer to their customers, the certificates that offer an account that the advertised capabilities are measurable items and the contracts that the CSPs offer to their customers, either being other CSPs or the cloud customer, including the list of any third party providers they collaborate.

We present here the implementation of this accountability support service through the execution of the cloud service selection process from the perspective of the cloud customer. As it is presented in Figure 3, the privacy expert of the cloud customer uses COAT tool, which allows this actor to select a cloud provider, satisfying a set of functional, security and privacy needs. These needs are the result of the

analysis performed by the privacy expert of the cloud customer to understand the company obligations, according to the legal norms and the regulatory framework of the country of business establishment, as well as the ethical obligations that the cloud customer is willing to adopt, based on what the company exhibits from a social perspective.

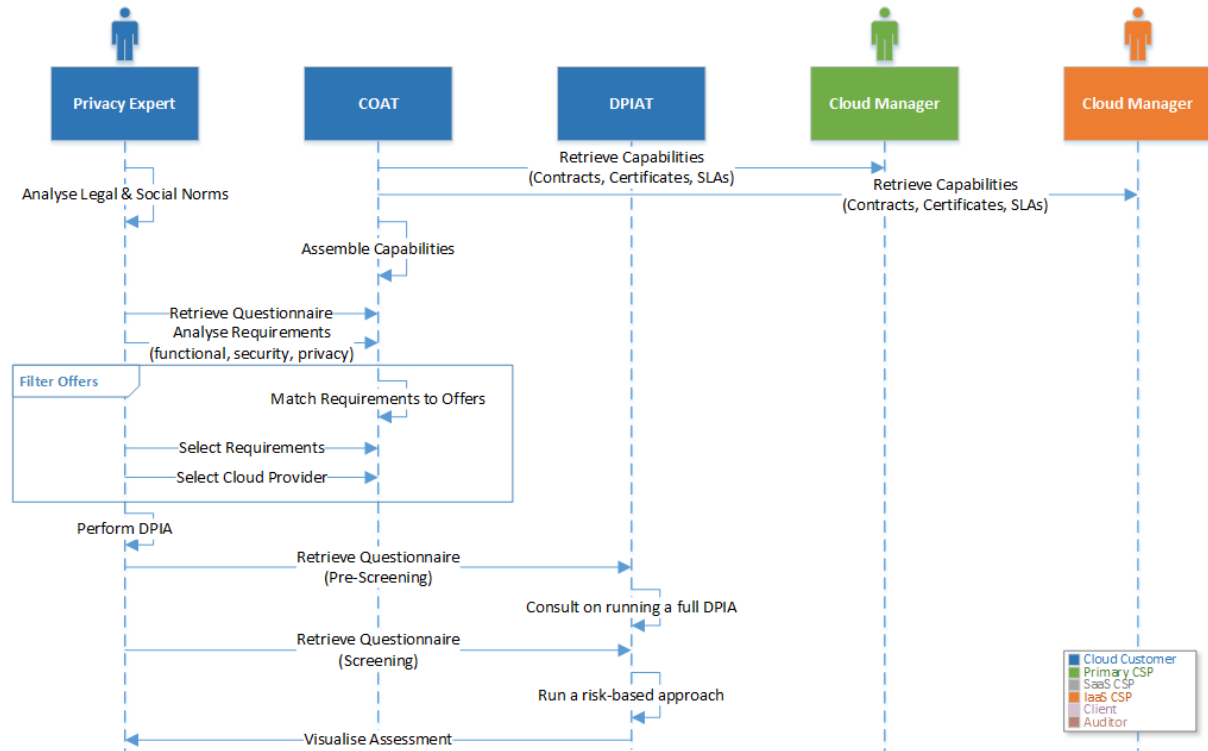


Figure 3: The interactions of the business actors in the policy definition and validation service – selection of a cloud service

COAT offers the privacy expert of the cloud customer a list of cloud service offers that match the stated requirements. In order to do so, COAT has already collected the relevant capabilities from the CSPs, including the ones from the cloud IaaS and SaaS providers of Figure 1. This Web-based tool enables the privacy expert to browse the capabilities of the various CSPs and, finally, select the primary CSP that fits to the requirements set for the cloud business.

The cloud service selection process must be validated through assisting the cloud customer in realising the risks stemming from their decision to run their business for the management of the personal data of their clients, using the service offered by the primary CSP. In that respect, the privacy expert of the cloud customer uses the DPIAT tool, as shown in Figure 1. The tool initially guides the cloud customer through a pre-assessment test on the need to run a data protection impact assessment process. In case that this is needed, the privacy expert uses DPIAT to load a set of 50 questions, which target to assess the cloud business project, the requirements for the collection and usage of the personal data of the clients, the storage and security requirements of the cloud business service, the restrictions on transferring information to third parties and other cloud specific questions. Through this approach, the DPIAT tool educates the privacy expert of the cloud customer about the risks arising from their decisions and how they can reduce these risks by selecting the primary CSP.

It must be noted that the process shown in Figure 3 can be followed by a CSP when they want to select the third party cloud providers to collaborate.

By selecting the primary CSP and their third party supply chain, the cloud customer needs to establish an agreement with them in order to start developing the software solution for the cloud business. As such, the privacy expert of the cloud customer communicates with the privacy officer of the primary CSP to define the relevant policies. The policy definition phase includes the interaction of the primary CSP and the cloud customer without the involvement of the A4Cloud tools, so that these actors agree on the functional, security and privacy prerequisites for running an instance of the cloud service for the cloud

customer business. This is achieved through a potential policy negotiation phase, the details on which are left outside A4Cloud. For our case, the interactions shown in Figure 4 are happening.

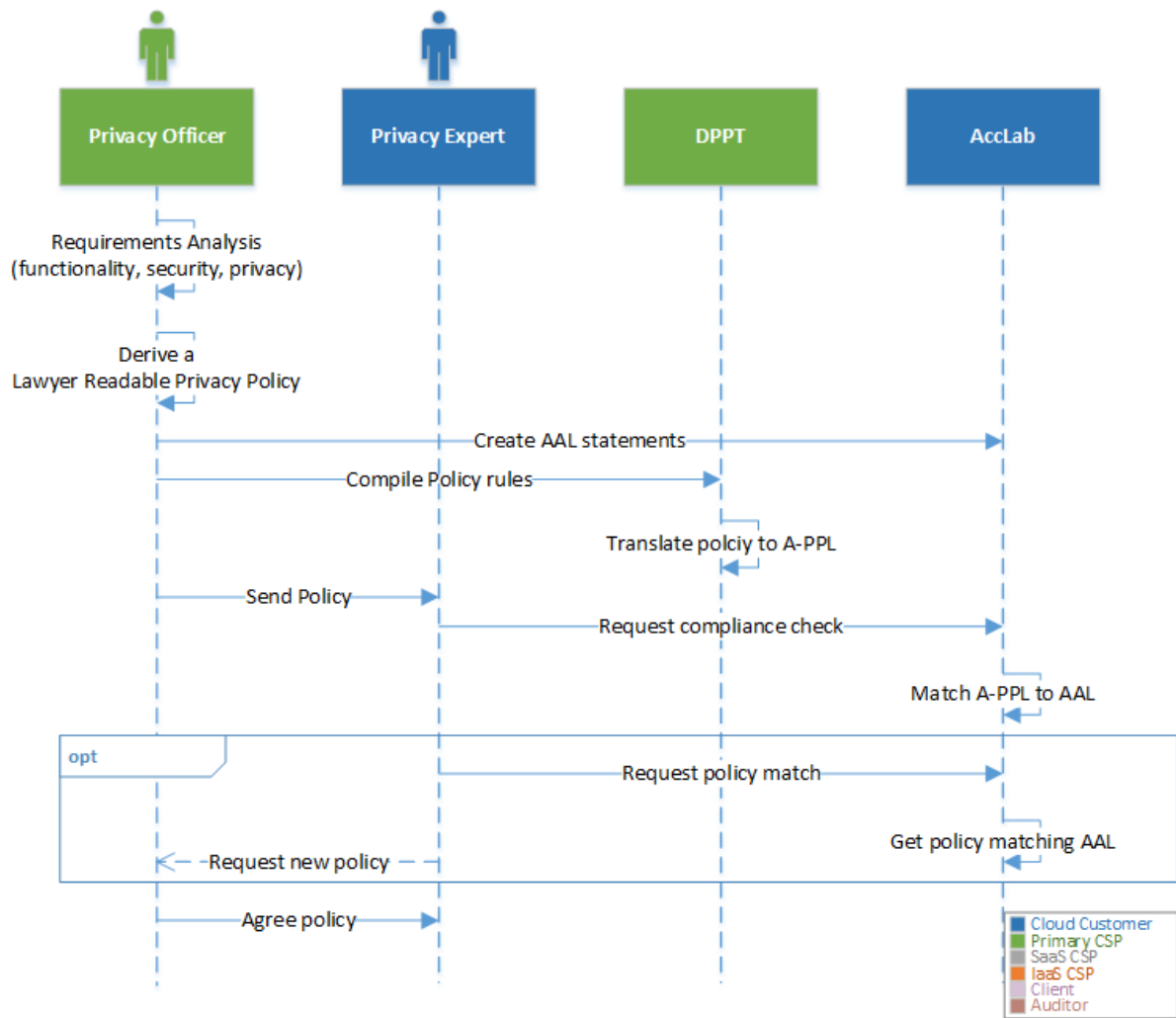


Figure 4: The interactions of the business actors in the policy definition and validation service – policy implementation

In detail, the privacy officer of the primary CSP is based on the lawyer readable policy agreement established with the representatives of the cloud customer to start developing the machine readable policies (in A-PPL format). This is achieved through DPPT, which offers a step-by-step approach to define the type of personal data involved in the policy, the access rights of the actors being involved in the business scenario and the rules for handling the events generated from the enforcement of the policy at runtime. In parallel, the primary CSP uses AccLab to describe their capabilities in an abstract language form (namely AAL).

As soon as a first version of the A-PPL policy is ready, it is communicated to the cloud customer. This actor uses AccLab to validate that the offerings of the policy match their preferences, as well as they comply with the claimed capabilities of the primary CSP for the provision of certain functional, security and privacy guarantees. In case that the cloud customer is not satisfied with the offered policy, the privacy expert communicates with the privacy officer of the primary CSP to request for modifications in the policy expressions.

2.3.2 Policy management and enforcement

Following the result of the previous accountability support service, in this one the use case application developers should emphasise on the configuration of the reference cloud environment and the

respective A4Cloud tools with the machine readable policies and the provision of an account from the CSPs for enforcement of these policies in their area of responsibility. This is presented in Figure 5

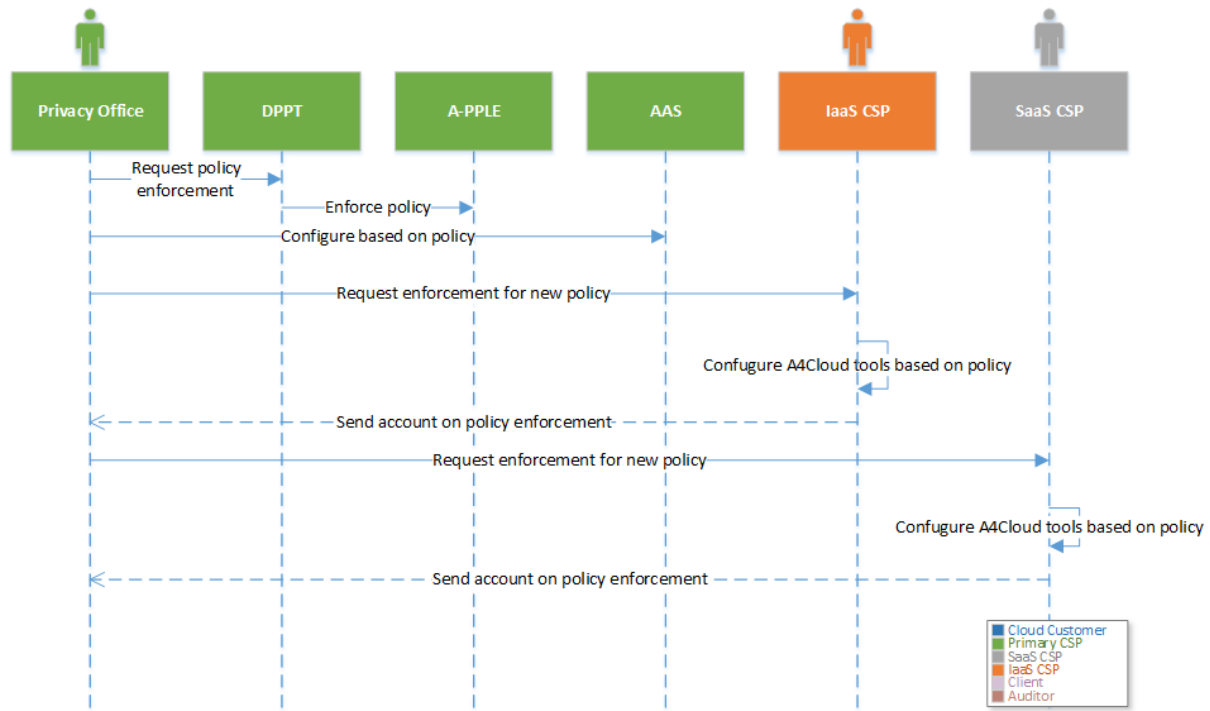


Figure 5: The interactions of the business actors in the policy management and enforcement service.

As shown there, the primary CSP is responsible for the configuration of their tools with the A-PPL policy and for making sure that the collaborating IaaS and SaaS CSPs are doing the same. Thus, the primary CSP prepares the instance of the cloud service, which is configured for the sake of the cloud customer, and deploys an instance of the A-PPLE and AAS A4Cloud tools, which are configured, according to the agreed A-PPL policy. It should be noted that the communication of the primary CSP with the other CSPs to manage the tool configuration process is performed manually without any tool support from A4Cloud.

Finally, the use case developers should ensure that the cloud service is properly operating at runtime, by allowing the cloud customer actors to perform actions, which trigger the enforcement of the policy rules, as expected.

2.3.3 Monitoring and environment state collection

In the monitoring and environment state collection accountability support service, we use the A4Cloud tools to generate logs on the enforcement of the A-PPL policies from the previous service or to collect such logs, which are generated in the various layers of the cloud protocol stack as a result of an action happening in the business application layer. This is presented in Figure 6.

Therefore, the primary CSP deploys an A-PPLE instance, which manages the enforcement of the policy rules and generates relevant logs. The events happening in the territory of the primary CSP are monitored by an AAS instance, which is also responsible for managing the monitoring activities when an interaction with the IaaS and SaaS CSPs is happening. In the territory of the other CSPs, the relevant instances of the AAS A4Cloud tool are responsible for monitoring the territory environment and collect logs from the various layers of the respective protocol stack. In case that the CSP is an IaaS, a DTMT instance is deployed in the environment of this CSP to monitor the networking layer and the events occurring there.

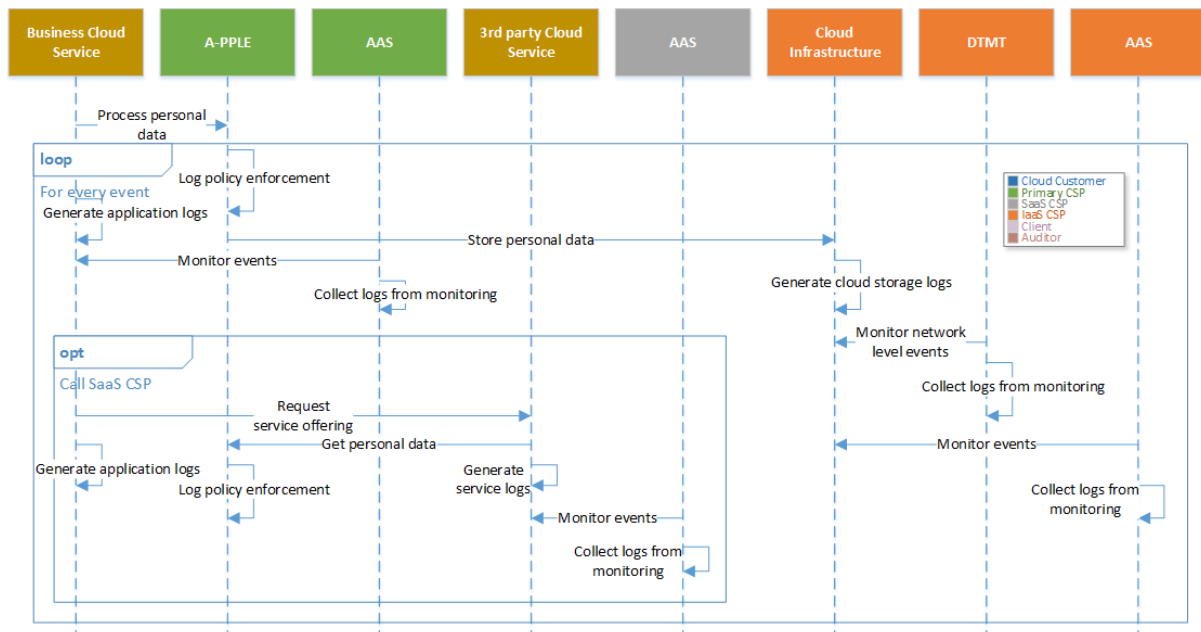


Figure 6: The interactions of the business actors in the monitoring and environment state collection service.

2.3.4 Collection and management of evidence

The collection of logs in the previous accountability support service is exploited in this service to allow the involved CSPs to manage the records of the logs, which can be eventually used as evidence to showcase the compliance of their data handling procedures with the agreed policies and the claimed capabilities. Figure 7 shows the interactions occurred in this service. As presented there, the collection and management of evidence is a process performed internally in every CSP. The process is coordinated by the AAS instance of each CSP, which collects the logs from various sources within the environment of the CSP and transforms them in an appropriate evidence format, which can be potentially used in the future as reference to what happened for a specific action of the cloud service.

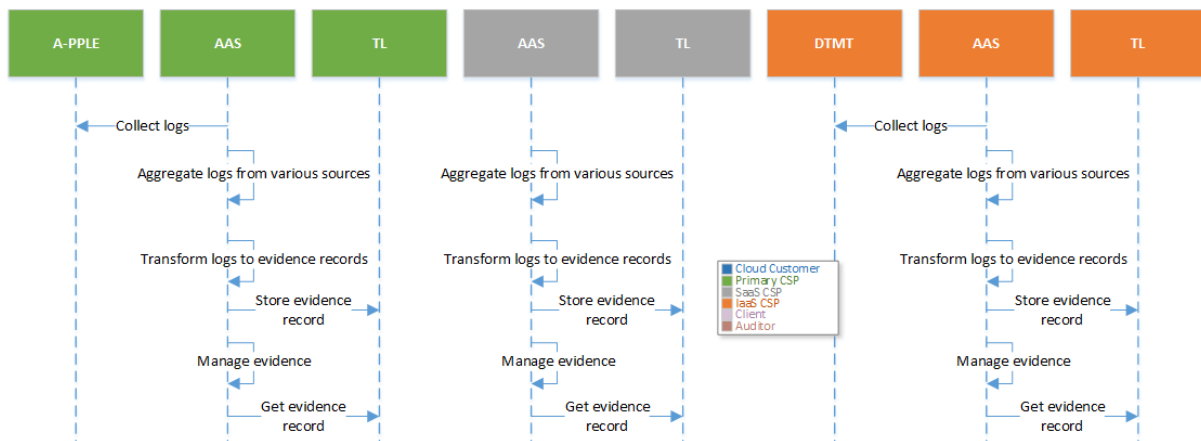


Figure 7: The interactions of the business actors in the collection and management of evidence service.

Depending on the type of the cloud model, the source of evidence can be the tools installed in each CSP territory, as shown in Figure 7. In all cases, the use case application developers should ensure that AAS deployment is configured, so that the embedded TL instance is the evidence repository to store the evidence records in a secure way.

2.3.5 Incident Management

Both the logs and the resulting evidence records can be used by the A4Cloud tools and the business actors to detect incidents in the reference cloud environment. As shown in Figure 8, an incident may be

raised from various tools and sources, depending on the incident nature and type. In all cases, the CSP maintains an instance of the IMT A4Cloud tool, which is responsible for collecting incidents and allowing the respective incidence management team to handle them. The developers should be aware that IMT has to be properly configured so that it receives incidents from other tools and be able to communicate these incidents, after they have been processed by the relevant incidence management team of the CSP, to the collaborating providers.

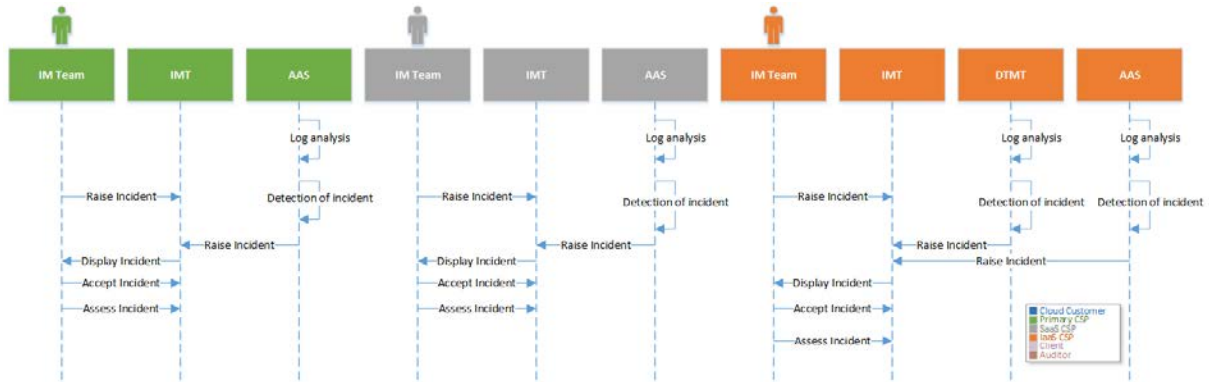


Figure 8: The interactions of the business actors in the incident management service.

In the example of Figure 8, the developers can realise that for the SaaS primary CSP the AAS instance can raise an incident or the incidence management team of the primary CSP can use IMT and register a perceived incident. In case of the IaaS CSP, apart from AAS, a DTMT instance can raise incidents that refer to data transfers occurring in the cloud infrastructure level of this CSP.

2.3.6 Notification

As soon as the IM team of a CSP assesses the severity of an incident, they have to undertake internal or external actions. More specifically, an incident has to be assessed from the IM team to decide whether it impacts the agreement made with other CSPs. In this case, a notification process has to be activated, according to the policy agreement rules, which have been used to configure the tools, as per the description in Section 2.3.2.

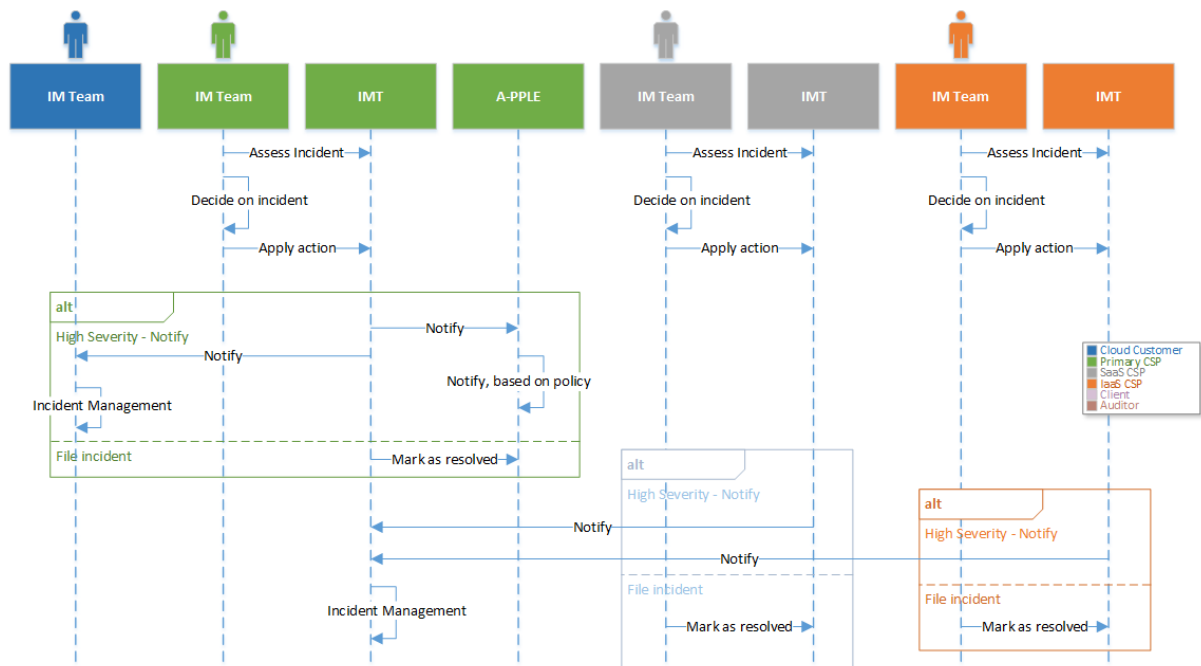


Figure 9: The interactions of the business actors in the notification service.

Figure 9 presents the implementation of the notification service for the reference cloud environment of Figure 1. The primary CSP has agreed with both the SaaS and IaaS provider that any incident affecting the cloud service offered by the primary CSP to the cloud customer must be notified to the IMT instance of the primary CSP. Through the implementation of this notification chain, all the incidents occurred in the cloud environment can be eventually notified to the cloud customer or the client, as we explained in the next section.

2.3.7 Remediation

In the implementation of the remediation accountability support service, we distinguish between the actions happening in the cloud environment and on the client's side. As such, in the cloud environment, the implementation of the remediation process follows an opposite direction than the notification one shown in Figure 9. This is presented in Figure 10, in which we showcase that the implementation of a remedy requested by an actor is attributed to the actor, which is direct communication with the requestor. Thus, when the cloud customer receives a notification on an incident, they can decide on which remedies must be applied (either actions handled internally or ones that should be performed from an external actor). Then, the cloud customer requests for a remedy from the primary CSP, which, in turn, may attribute this request to other CSP or apply it in collaboration with another CSP. The use case application developers should note that the interactions shown in Figure 10 are not supported by any A4Cloud tool.

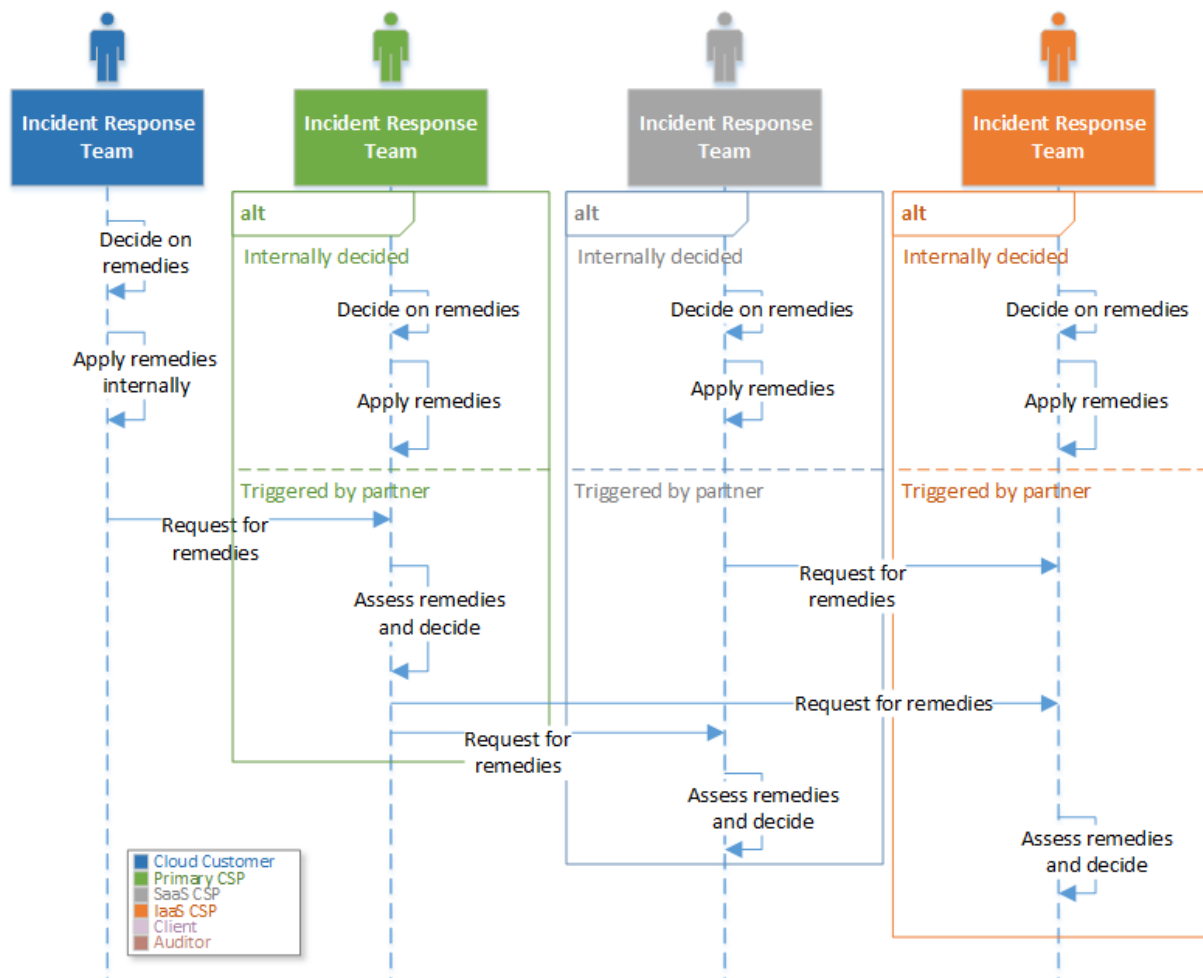


Figure 10: The interactions of the business actors in the remediation service – the cloud environment perspective.

In case that a notification has reached the clients of the cloud customer (see Figure 11), the remediation process is supported by RRT. This is a Web-based tool provided by A4Cloud, which is integrated into DT and is responsible for visualising the notifications to the clients' device, along with a list of suggestions, in response to these notifications. As shown in Figure 11, the clients interact with RRT and

they can finally decide to the appropriate remedies, which can take the form of communication with a cloud supervisory authority or a request to a redress action in the cloud environment, like the deletion of personal data affected by the incident, referred in the notification.

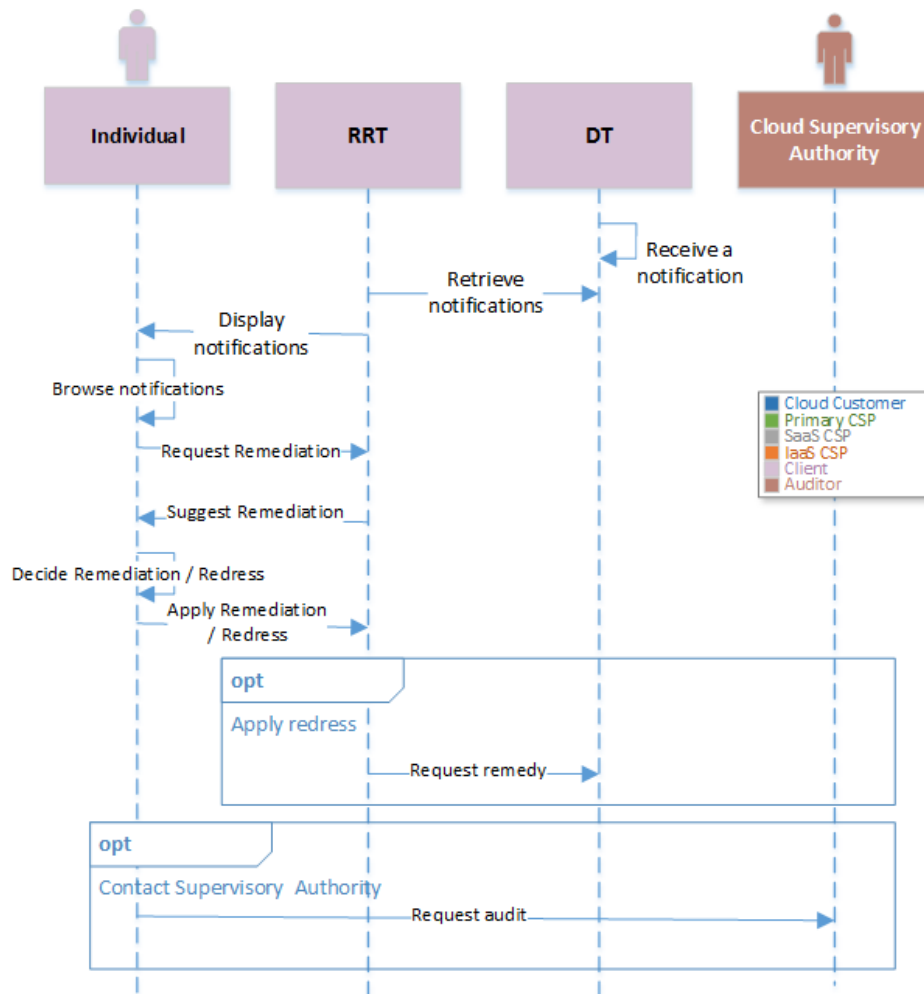


Figure 11: The interactions of the business actors in the remediation service – the client perspective.

The developers should be aware that the implementation of redress is handled through DT and must have been implemented from the relevant cloud actor. For example, if the redress refers to a data deletion case, DT should be able to access the relevant service interface from the A-PPLE instance of the primary CSP.

2.3.8 Validation

The validation accountability support service refers to both the cloud service providers and customers and the clients. All these roles must be able to get evidence that the agreed policies are properly reflected in the data handling procedures of the business actors. The validation may involve cloud auditors who perform external audits to the business actors.

More specifically, in this service, the privacy experts and officers of the business organisations may request for an audit to the collaborating cloud providers. The audit is performed through the relevant AAS instance of the organisation to be audited either by the privacy expert / officer of the external actor that requests the audit or a cloud auditor. This is shown in Figure 12.

Apart from external audit, the organisations may use their AAS instance to perform internal audits, as well, as a proactive measurement to test their compliance to accountability practices.

The application developers should pay attention to the use of the TL instance for each client, which allows the secure communication of the DT instance of each individual with the A-PPLE instance of the primary CSP.

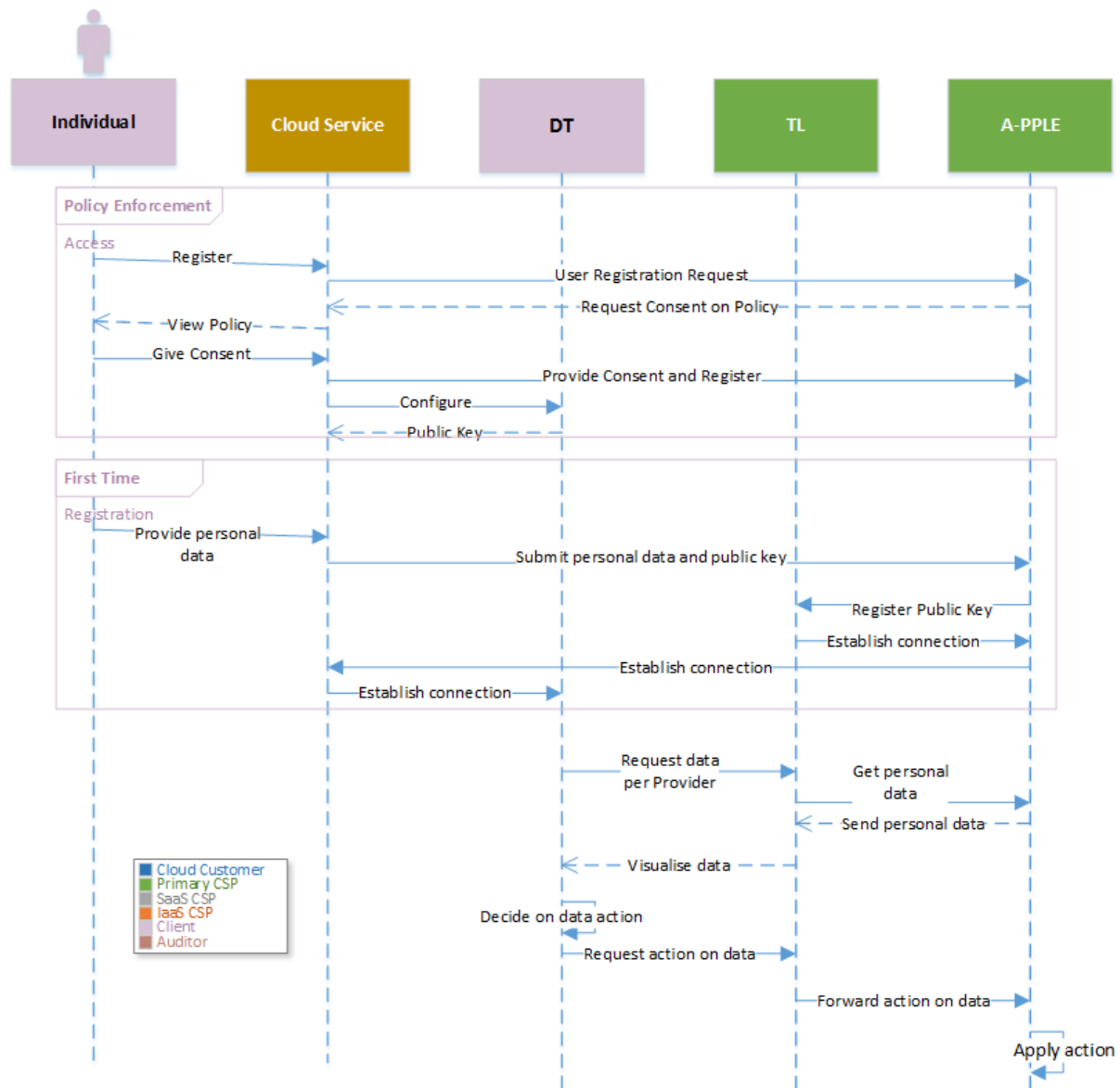


Figure 13: The interactions of the business actors in the validation service – data subject enablement

2.4 Summary of the tools usage

We summarise in this section the use of the A4Cloud tools per business actor and how they are implementing the relevant accountability support service. The summary includes the use of the tools as it was presented in Section 2.3, but it makes references to scenarios, in which the A4Cloud tools can also be exploited, like the selection of a CSP from another CSP. This analysis is presented in Table 1.

Table 1: Use of the A4Cloud tools per business actor, taking a specific accountability role

Accountability Support Service	Actor	Tool	Used in Reference Environment ¹	Can be used in an extended scenario
Policy Definition and Validation	Cloud customer	COAT	Select the primary CSP, based on functional, security and privacy requirements	-

¹ As shown in Figure 1

Accountability Support Service	Actor	Tool	Used in Reference Environment ¹	Can be used in an extended scenario	
		DPIAT	Assess the impact of the primary CSP selection on the data protection aspects, and get the requirements to follow specific privacy, security and functional steps	-	
		DPPT	-	If a cloud customer being a data controller has ICT resources to host an A-PPLE instance	
		AccLab	Check policy compliance to their requirements and match the policy to primary CSP capabilities (and their third parties)	-	
	Cloud service provider	COAT	-	If a CSP needs to select a third party cloud provider	
		DPIAT	-	If a CSP needs to assess the impact from the selection of a third party cloud provider	
		DPPT	Define accountability policies for the cloud customer in A-PPL	-	
		AccLab	-	If a CSP requests a policy agreement with another CSP	
	Policy Management and Enforcement	Cloud customer	DPPT	-	If a cloud customer being a data controller has used DPPT to define policies
			A-PPLE	-	If a cloud customer being a data controller has ICT resources to host an A-PPLE instance
AAS			-	If a cloud customer being a data controller has ICT resources to host an A-PPLE instance	
IMT			-	If a cloud customer being a data controller has ICT resources to host an IMT instance	

Accountability Support Service	Actor	Tool	Used in Reference Environment ¹	Can be used in an extended scenario
	Cloud service provider	DPPT	For SaaS CSP, submit agreed policy to the A-PPLE instance	-
		A-PPLE	For SaaS CSP, enforce policy rules, once receiving application level requests from the cloud service business	-
		AAS	Configure monitoring cloud protocol stack, based on agreed policy	-
		IMT	Configure notification providers and subscribers, based on agreed policy	-
		DTMT	For IaaS CSP, configure monitoring networking layer, based on agreed policy	-
	Client	DT	Once the client requests to register into the cloud service by giving consent to the provided policy, DT is configured to monitor disclosures for primary CSP	-
Monitoring and Environment State Collection	Cloud customer	A-PPLE	-	If a cloud customer being a data controller has ICT resources to host an A-PPLE instance
		AAS	-	If a cloud customer being a data controller has ICT resources to host an A-PPLE instance
	Cloud service provider	A-PPLE	The primary SaaS CSP generates policy enforcement logs	A SaaS CSP in the chain uses A-PPLE for downstream usage
		AAS	A CSP collects logs from the layers of the cloud protocol stack	-
		DTMT	An IaaS CSP monitors the networking layer of the cloud protocol stack and generates logs	-
Collection and Management of Evidence	Cloud customer	AAS (and embedded TL)	-	If a cloud customer being a data controller has ICT resources to collect logs

Accountability Support Service	Actor	Tool	Used in Reference Environment ¹	Can be used in an extended scenario
	Cloud service provider	AAS (and embedded TL)	Collect logs, transforms to evidence records and stores them in a secure way	-
		DTMT	For IaaS CSP, it allows collection of logs generated from the monitoring of the network part of an IaaS infrastructure	-
Incident Management	Cloud customer	IMT	-	If a cloud customer being a data controller has ICT resources to deploy an IMT instance
	Cloud service provider	IMT	Receive incidents or allow human actors to manually register incidents and handle them	-
		AAS	Analyse logs and records to raise incidents on policy violations and security breaches	-
		DTMT	For IaaS CSP to analyse logs to raise incidents on data transfers	-
Notification	Cloud customer	IMT	-	If a cloud customer being a data controller has ICT resources to deploy an IMT instance
		A-PPLE	-	If a cloud customer being a data controller has ICT resources to deploy an A-PPLE instance
	Cloud service provider	IMT	Allow human actors to notify other organisations on incidents affecting their agreements and contracts	-
		A-PPLE	Allow the primary CSP to notify clients, based on policy	-
Remediation	Client	RRT	Present remediation options for notifications related to incidents	-
		DT	Act as mediator in the remediation process	Enforce redress actions
Validation	Cloud customer	AAS	Perform audits to primary CSP	If a cloud customer being a data controller has ICT

Accountability Support Service	Actor	Tool	Used in Reference Environment ¹	Can be used in an extended scenario
				resources to perform internal audits
	Cloud service provider	AAS	Perform internal and external audits	-
	Cloud Auditor	AAS	Perform audits to CSPs	If a cloud customer being a data controller has ICT resources to perform audits to cloud customer
	Client	DT	Control the disclosure of personal data in the primary CSP	-

3 Updates on the specifications for the wearables use case

This section exploits the guidelines for use case developers in Section 2 to provide a practical example on how they have been used for the development of the wearables use case, which was introduced in Deliverable D47.1.

3.1 Overview of the wearable service

In this section, we make an overview of the wearables use case to develop and operate the wearable service, as it has been introduced in [2]. As such, we re-introduce the Wearable Co, an SME, which is the manufacturer of wearable devices and wants to offer an application (the Wearable Service), through a Web-based cloud environment, that will enable the clients to control the data collected by these devices and get customisable visualisations of their wellbeing status.

Figure 14 makes a reminder of the business perspective for the wearables use case. The wearable service is supported by the cloud service chain shown in this figure. Kardio-Mon is the primary cloud service provider, which establishes a business relationship with the Wearable Co to implement this cloud service on behalf of the Wearable Co. Kardio-Mon is thus the connecting actor between the providers of the cloud service supply chain and the Wearable Co, which is the cloud customer. The providers in the supply chain are realised through the business interaction of Kardio-Mon with Map-on-Web and DataSpacer. Each of these providers serve a specific set of cloud functionalities, which eventually facilitate the interaction of the Wearable Co with the cloud providers. In other words, the respective service and infrastructure providers serve the wearable service and the actors that will operate and consume this application. As such, Figure 14 presents the relationship between these actors and the flow of the information in order to deliver the Wearable Service to the appointed customers.

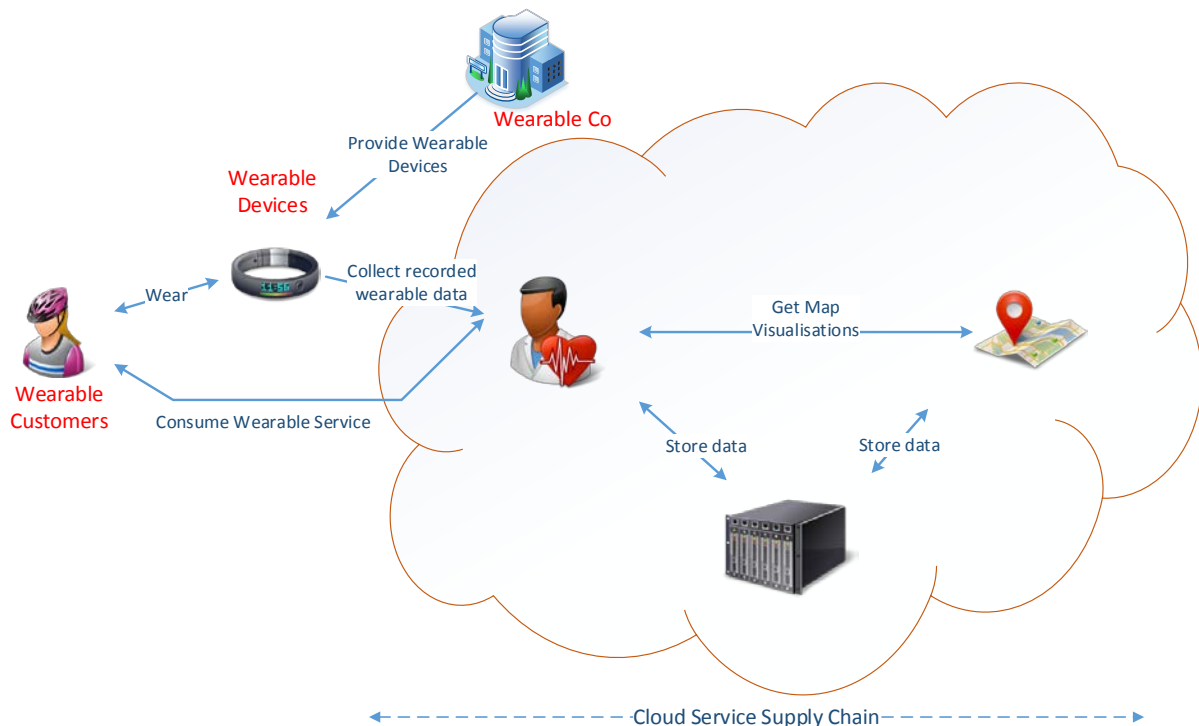


Figure 14: The use case overview for the Wearable Service – the Business Perspective

The Wearable Co sells the respective wearable devices to their customers, who may access the wearable service through either these devices, which collect personal data and submit them the cloud application, or the Web application deployed by Kardio-Mon in order to manage the collected and process personal data.

We note that the implementation of the wearables service application has not changed since the previous version in D47.1 and, thus, it is not repeated in this deliverable.

It must be highlighted that from, this point forward, the analysis of the use case emphasises on the time that the Wearable Co starts the investigation for the operation of a cloud business, like the wearable service, which is already in the market by Kardio-Mon.

3.2 The accountability-based analysis of the Wearable Service

As already presented in [2], the actors in this use case take a specific role in the cloud computing and the data protection domains. Given that the wearable service as a cloud service is provided by Kardio-Mon and is customised as a service instance for the sake of the Wearable Co, the mapping of the use case actors to roles takes the form of Table 2.

Table 2: The assignment of roles to the actors of the Wearable Service Use Case

Wearable Service Actor	Short Business Description	Cloud Computing Role	Data Protection Role
Wearable Co Customer	The end user of the Wearable Co accessing the particular instance of the Wearable Service	Individual Cloud Subject	Data Subject
Wearable Co	The SME operating the Wearable Service instance	Organisational Cloud Customer	Data Controller
Kardio-Mon	A SaaS SME cloud provider offering the Wearable Service	Cloud Provider	Data Processor
Map-on-Web	A SaaS cloud provider allowing the creation of map visualisations for the statistical analysis of the collected personal data	Cloud Provider	Data Processor
DataSpacer	An IaaS cloud provider operating an OpenStack-based cloud environment for processing and hosting different types of data	Cloud Provider	Data Processor

In the list of actors and roles presented in Table 2, we must consider at least one additional actor, which takes the role of the Cloud Auditor and/or the Supervisory Authority.

Each actor in the wearable service use case must address the functional elements of the accountability lifecycle, presented in Figure 2. Therefore, during the instantiation of the Accountability framework for the wearable service use case, all the actors should go through the lifecycle phases and demonstrate how they follow the respective functional elements, by adopting accountability practices and implementing respective accountability mechanisms.

In the next paragraphs, we present the adoption of the lifecycle for the actors involved in this use case.

3.2.1 The accountability lifecycle for the Wearable Co

The Wearable Co is a cloud customer that acts as a data controller and regulates the type of data to be collected from the Wearable Co Customers, the purpose for doing so and the accountability policies under which this data will be processed and stored in the cloud.

This cloud customer, acting as controller, runs the processes allocated to the phases of the Accountability lifecycle in order to adopt an accountable attitude in the provision of their business, including personal data.

Embrace responsibilities

In this phase, the Wearable Co needs to document the obligations that this actor should accept in order to run the instance of the wearable service. These obligations refer both to business and compliance type relationships. In that sense, the Wearable Co investigates on the responsibilities towards their customers and the involved cloud providers as well, by analysing the legal requirements, the social norms, the organisational values and the ethical behaviour in order to offer this wearable service, using resources from the cloud providers in an accountable way. The Wearable Co should be able to understand the potential implications from their failure in addressing properly these obligations. The Wearable Co should also exhibit the appropriate readiness to demonstrate to the Cloud Auditor their compliance to these obligations both against their customers and the collaborating cloud providers.

The Wearable Co should be proactive enough in the accountability domain at all layers of the organisational structure. They should define governance processes for the acceptance of the organisation responsibilities for the protection of personal data involved in the wearable service and the provision of the necessary means for the collaboration with cloud providers. These processes must clearly define the means that the Wearable Co deploys to fulfil their obligations and how the responsibilities and the actions to be taken are integrated across the organisational structure.

The governance processes span across the lifecycle phases and include the definition of techniques and tools that assist the Wearable Co in demonstrating their compliance to accepted obligations. The demonstration target refers to:

- The Wearable Co Customer, who must be able to verify the compliance of the Wearable Co in:
 - Selecting and managing Kardio-Mon, as the primary cloud provider and their third party collaborators Map-on-Web and DataSpacer;
 - Ensuring the integrity of the operational phase of their business;
 - Preparing their internal resources in discovering and handling exceptional events, as they are reported to them from the cloud providers.
- The Wearable Co itself, who must be able to assure their compliance to obligations through running continuous verification of their practices to operate the wearable service;
- The cloud auditor, who must be able to perform validation and auditing on the claimed practices, techniques and methods.

The Wearable Co must understand which are the risks associated with their decision in requesting the specific personal data from the Wearable Co Customers, as well as the risks from the intention of the Wearable Co to deliver the wearable service in collaboration with Kardio-Mon, Map-on-Web and DataSpacer.

Define Policies

In this phase, the Wearable Co enters the design and implementation stage of the wearable service. To this end, the Wearable Co must detail the functionality and the associated non-functional requirements of the instance of the wearable service they want, which lead to the conduction of a risk and impact assessment for the personal data linked to this cloud service. The analysis entails the requirements in the accountability domain that they have already been investigated in the previous phase and allow this SME to perform a risk analysis on the processing of the personal data collected from the Wearable Co Customer, using the resources provided by Kardio-Mon and their third parties (Map-on-Web and DataSpacer). This risk analysis is joint with an impact assessment that refers to the consequences of the decision of the Wearable Co to deal with the involved risks. The process for the Wearable Co includes the definition and maintenance of controls, in response to the identified risks, and the monitoring of a quantified risk treatment plan.

In this phase, the Wearable Co has to properly select the cloud provider actor(s) to collaborate. This means that it identifies the required resources and assets from the cloud providers and analyses their certifications and claimed contract provisions. In that respect, the Wearable Co must be able to conduct audits to mainly Kardio-Mon, in order to validate their functionality and compliance to obligations.

The subsequent step in this phase is the compilation of accountability contract between the Wearable Co and Kardio-Mon. This contract documents in detail what is provided in the instantiation of the wearable service, including the access and usage control rules on the personal data disclosed by the potential Wearable Co Customers, time constraints about personal data collection (data retention period), the processing data location and transfers, the clauses that allow a cloud auditor for auditability, the rules for facilitating reporting and notification from Kardio-Mon towards primary the Wearable Co

and subsequently if needed the Wearable Co Customers, and any redress recommendations that the Kardio-Mon should implement in case of failures.

Enforce Policies

In this phase, the Wearable Co requests the enforcement of the contract agreed with Kardio-Mon through tool support. In that respect, the Kardio-Mon should provide an account to the Wearable Co for the demonstration of their effectiveness in meeting the provisions of the contract at the operational level.

This contract should also be the basis for the Wearable Co to offer an accountability policy to their customers, in which the customers could be able to express certain privacy related preferences and give consent about the use of their personal data by whom and under which conditions.

Monitor Practices

In this phase, although the Wearable Co does not perform any monitoring activities, they are responsible for handling any complaints filed by their customers to the normal operation of the instance of the wearable service.

Correct Violations

In this phase, the Wearable Co is responsible for handling exceptions occurred in the cloud environment and reported to them through Kardio-Mon. Thus, this actor shall notify the Wearable Co customers about these incidents and propose appropriate remediation actions. In case of exceptional criticality of the incident, this must communicate it to the cloud auditor, as per the dictations of the regulatory framework. The Wearable Co is responsible for demonstrating to the cloud auditor actor their compliance to the accountability policy offering the customers about the attribution of failures.

Furthermore, in the tasks of the Wearable Co are:

- Request for audit on Kardio-Mon on their compliance to the accountability contract for attributing failures;
- Request for the application of specific redress actions from Kardio-Mon.

Demonstrate Compliance

In this phase, the Wearable Co shall be able to allow other cloud actors, such as Kardio-Mon and the auditors, to request for an account for validating their operations. They should also perform external verification through audits that periodically assess the adopted practices and ensure the alignment with the results of previous internal and external audits.

3.2.2 The accountability lifecycle for Kardio-Mon

Kardio-Mon is a cloud provider that acts as a data processor. The processing of personal data is performed in line with the accountability policies agreed with the Wearable Co.

Embrace responsibilities

In principle, this phase precedes the time that the Wearable Co wants to operate a cloud service for managing data from the wearable devices. It refers to the time that Kardio-Mon enters the cloud market with the proposal solution based on the wearable service. However, the activities in this phase may also refer to the case that Kardio-Mon wants to establish an additional collaboration with another cloud provider, which implements some extra functionality for the instance of the wearable service that targets the Wearable Co. In this case, Kardio-Mon may act as a data controller and follow the activities presented in the respective phase for the Wearable Co.

Define Policies

In this phase, Kardio-Mon enters the design and development phase for the provision of the wearable service instance to the Wearable Co. The analysis performed in this phase considers the requirements from the cloud customer and leads Kardio-Mon to the proposition of a specific contract for the Wearable Co, as explained in section 3.2.1.

In case that Kardio-Mon needs to establish an additional collaboration with another cloud provider, then this phase involves also the steps for selecting cloud providers and performing a data protection impact assessment on this choice.

Enforce Policies

As soon as a contract has been agreed between Kardio-Mon and the Wearable Co, the enforcement of the contract terms in the technical means of Kardio-Mon and the other providers of the cloud service chain is applied. Thus, in this phase, Kardio-Mon requests an account from the other cloud providers, namely Map-on-Web and DataSpacer, on their preparedness to address the contract terms and, then, offers an account to the Wearable Co on the effectiveness of the specific wearable service instance to run as expected.

Monitor Practices

In this phase, Kardio-Mon activates the necessary processes to monitor the execution of their cloud service and collect and store information about this operation. Thus, Kardio-Mon uses the appropriate tools to implement the monitoring of the wearable service from a security perspective. The activities involve the analysis of the collected information and the compilation of this information to constitute evidence for the behaviour of the various elements of the wearable service. In that respect, Kardio-Mon must be able to monitor and collect events about the enforcement of accountability related security properties in their regime, with respect to the operation of the Wearable service. The events may refer to both the proper operation of the service as well as the incidents that may raise an abnormal behaviour of the Kardio-Mon environment. The events can take the form of logs about the enforcement of data access rules applied to the service, the implementation of controls for the deletion of data after the expiration of the data retention period, etc.

Since Kardio-Mon is a SaaS cloud provider, the collection of logs refers to the monitoring of the events happening in the upper layers of the cloud protocol stack. The collection of logs is supported by tools, which compile the logs into evidence records for further use in case of auditing. Kardio-Mon needs to deploy tools for the management of these logs according to specific integrity, confidentiality and access control requirements.

Correct Violations

In this phase, Kardio-Mon is responsible for the implementation of mechanisms for the detection of exceptions occurred in the cloud environment, which may refer to potential security breaches or policy violations. These exceptions refer to incidents identified by the tools deployed by Kardio-Mon. They should also refer to notifications, received from the Map-on-Web and/or DataSpacer, about incidents identified by the tools deployed in the regime of these cloud providers, which have been assessed as security breaches or violations by the authorised actor(s) in this provider.

Upon the detection of an incident or the receipt of a notification about an incident, Kardio-Mon must implement the process for the assessment of the incident, examining its severity and decide on the implementation of two complementary ways:

- i. Develop the notification chain: in this case, Kardio-Mon decides which incident(s) should be notified to the Wearable Co for further assessment and if there is an urgent need for sending notifications directly to the Wearable Co customers or any Supervisory Authority.
- ii. Support the implementation of remediation actions: in this case, Kardio-Mon activates the necessary security controls to mitigate the risks arising from the propagation of the incident in their cloud business. The decision on the selection of controls is subject to the severity of the detected incidents.

We also classify the following actions among the tasks of Kardio-Mon to be executed in this phase:

- Request for audit on Map-on-Web or DataSpacer on their compliance to the accountability contract(s) for attributing failures;
- Request for the application of specific redress actions from Map-on-Web or DataSpacer.

Demonstrate Compliance

In this phase, Kardio-Mon shall be able to allow the Wearable Co or even other cloud actors, such as Map-on-Web and the cloud auditors, to request for an account for the validation of the Kardio-Mon operations towards addressing the agreed policies/contracts and the applicable regulations.

3.2.3 The accountability lifecycle for Map-on-Web

Map-on-Web is a cloud provider that acts as a data processor. The processing of personal data is performed in line with the accountability policies agreed with Kardio-Mon.

Embrace responsibilities

As in the case for Kardio-Mon, this phase precedes the time that the Wearable Co establishes an agreement with Kardio-Mon to operate the wearable service. It refers to the time that Map-on-Web enters the cloud market with the proposal solution for the map visualisation of large datasets. Thus, the activities in this phase may refer to the case that Map-on-Web accepts in the implementation of the appropriate processes to support the operation of the wearable service in an accountable manner.

Define Policies

This phase precedes the time that the Wearable Co establishes an agreement with Kardio-Mon to operate the wearable service. It refers to the case that Map-on-Web compiles a policy to be agreed with Kardio-Mon.

Enforce Policies

Again, the enforcement of the policies agreed between Map-on-Web and Kardio-Mon precedes the time that the Wearable Co enters into the business for the wearable service. However, this phase may relate to the activities of Map-on-Web to enforce an instance of the agreement with Kardio-Mon for the case of the wearable service.

Monitor Practices

In this phase, Map-on-Web has already activated the necessary processes to monitor the execution of their cloud service and collect and store information about this operation. Thus, Map-on-Web uses the appropriate tools to implement the monitoring of the interaction with Kardio-Mon to produce map visualisations for large datasets submitted by Kardio-Mon. The monitoring process happens on all the SaaS layers of the cloud protocol stack.

The implementation of the activities in this phase is similar to the one presented in section 3.2.2 for Kardio-Mon.

Correct Violations

In this phase, Map-on-Web implement the accountability mechanisms like the ones deployed for Kardio-Mon. Thus, Map-on-Web detect exceptions occurred in the cloud environment of their SaaS business and assess the severity of the incidents to determine where a notification of the incident should be reported to Kardio-Mon. Among the other tasks of Map-on-Web in this phase, this actor requests for audit on DataSpacer on their compliance to the accountability contract(s) for attributing failures.

Demonstrate Compliance

In this phase, Map-on-Web shall be able to allow Kardio-Mon or any other cloud provider and customer to request for an audit for the validation of the operations running by Map-on-Web towards addressing the agreed policies/contracts and the applicable regulations.

3.2.4 The accountability lifecycle for DataSpacer

DataSpacer is an IaaS cloud provider that acts as a data processor for both Kardio-Mon and the Map-on-Web. The processing of personal data is performed in line with the accountability policies agreed with these two providers.

Embrace responsibilities

As in the case for Map-of-Web, this phase precedes the time that the Wearable Co establishes an agreement with Kardio-Mon to operate the wearable service. It refers to the time that DataSpacer enters the cloud infrastructure market to offer storage and processing facilities to SaaS and PaaS providers. Thus, the activities in this phase may refer to the case that DataSpacer accepts in the implementation of the appropriate processes to support the operations offered by Kardio-Mon and Map-on-Web in an accountable manner.

Define Policies

This phase precedes the time that the Wearable Co establishes an agreement with Kardio-Mon to operate the wearable service. It refers to the case that DataSpacer compiles their capabilities to support data storage in specific geographical area and with certain security mechanisms applied (i.e. level of data encryption, etc.).

Enforce Policies

The enforcement of policies on the DataSpacer side precedes the time that the Wearable Co enters into the business for the wearable service. However, this phase may relate to the activities of the DataSpacer to enforce an updated policy instance for the support of the operations by Kardio-Mon or Map-on-Web.

Monitor Practices

DataSpacer has already activated the necessary processes to monitor the execution of their cloud service and collect and store information about this operation. DataSpacer uses the appropriate tools to implement the monitoring of the interaction with Kardio-Mon and Map-on-Web for storing data in their infrastructure. The monitoring of the activities in this phase is similar to the one presented in section 3.2.2 for Kardio-Mon and this process refers to events happening in the lower layers of the protocol stack.

Correct Violations

In this phase, DataSpacer implement the accountability mechanisms to detect exceptions occurred in the cloud environment of their IaaS business. These exceptions mainly refer to potential violations on data transfer policies. DataSpacer is responsible for assessing the severity of the incidents and activate the notification to Kardio-Mon and/or Map-on-Web. Among the other tasks of DataSpacer in this phase, this actor is responsible for the implementation of controls in response to the raised incidents about data transfer policy violations.

Demonstrate Compliance

In this phase, DataSpacer shall be able to allow Kardio-Mon, Map-on-Web or any other cloud provider and customer to request for an audit for the validation of the operations running by DataSpacer towards addressing the agreed policies/contracts and the applicable regulations.

3.2.5 The accountability lifecycle for the Wearable Co Customer

The Wearable Co Customer is the end user of the wearable service, thus the client of the Wearable Co. This actor takes the role of a cloud / data subject, who agrees to share their personal information with the cloud provides involved in the provision of the wearable service.

This actor does not follow the accountability lifecycle, but it benefits from the adoption of this cycle by the other cloud roles, as described in the previous sections. However, the involvement of the Wearable Co Customer in the execution of the lifecycle from the perspective of the other roles is important, because the Wearable Co Customer:

- May be able to affect the policy definition phase by submitting their preferences for certain data protection options, like maximum data retention time, allowable geographical locations for data storage, etc.
- Should give their consent to the enforcement of the policies published by the Wearable Co for the use of the wearable service, prior to the engagement with this service.
- Should be able to validate the data handling practices of the Wearable Co and the collaborating cloud service providers for the management of their disclosures according to the policies.
- Should be able to receive notifications about the detection of incidents affecting their privacy in the cloud environment.
- May ask for an audit to the Wearable Co or any other cloud role in response to a perceived or reported incident.

4 Implementation of the final prototype

This section takes advantage on the presentation of the wearables use case in Section 3 and elaborates on how the Cloud Accountability Reference Architecture has been instantiated for this scenario and the business actors shown in Table 2.

4.1 Instantiating the Cloud Accountability Reference Architecture for the wearables use case

This section presents the instantiation of the Cloud Accountability Reference Architecture (CARA), as it has been described in WP42 and Deliverable D42.4 [3]. More specifically, we focus on how CARA is instantiated to explain the implementation of accountability across the actors of the wearables use case. In that respect, it presents the adoption of the accountability support services and the respective accountability artefacts from each actor of Table 2 and elaborates on the perspectives of the (preventive, detective and corrective) phases of the accountability mechanisms, explaining the use of the relevant A4Cloud tools.

4.1.1 The perspective of the Wearable Co

From the analysis presented in Section 3.2.1, the Wearable Co needs to implement the following accountability support services.

Policy Definition and Validation

In the *Policy Definition and Validation* accountability support service, the Wearable Co requires the A4Cloud tools to:

- Get a guided selection of a cloud provider, according to functional, security and privacy requirements;
- Assess the impact of the cloud provider selection on the data protection aspects, and get the requirements to follow specific privacy, security and functional steps;
- Perform policy matching between abstract policy statements and preferences.

In more detail, during the execution of the policy definition and validation service, the Wearable Co analyses the obligations of the organisation as they are stemming from the applied regulations in the country / area, in which this established organisation decides to start their online business, as well as the type of this business and the involved data. The obligations may also reflect the need of the Wearable Co for respecting or accepting a set of socially expressed norms. A4Cloud supports the Wearable Co in this service by offering the COAT tool. The tool is used by a data protection, policy or security expert of the Wearable Co for getting a guided selection of Kardio-Mon among other cloud providers, which exhibit similar functional, security and privacy characteristics.

The Wearable Co can validate the selection of Kardio-Mon in terms of actually addressing the advertised capabilities and assessing the impact of this selection in the data protection practices adopted by the Wearable Co. This is a mandatory action to be undertaken by the Wearable Co subject to the provisions of the new General Data Protection Regulation. As such, A4Cloud offers DPIAT, which is used by the data protection or the security expert of the Wearable Co to perform a data protection impact assessment. This is a questionnaire-like assessment, which requires the respective actor to answer a set of questions in order to evaluate the data protection risks related to their decision to select Kardio-Mon for running their cloud business.

Through DPIAT, the Wearable Co can determine the operational capacity of Kardio-Mon to effectively address the privacy, security and functional requirements of the Wearable Co, through a risk-based approach. In this case, the Wearable Co has to validate their selection on a Kardio-Mon by performing an impact assessment process for the protection of the personal data of their Wearable Co clients. The Wearable Co analyses and has access to the same accountability assets, as in the case of the use of the COAT tool, and they also access the Certificates and Assessments of the cloud provider to validate their claimed assets.

In this accountability support service, the Wearable Co is also able to validate the suggested by Kardio-Mon accountability policies, which reflect the instantiation of the Kardio-Mon security and privacy capabilities for the sake of the Wearable Co requirements. In that respect, the Wearable Co uses the

AccLab tool provided by A4Cloud, which enables them check that the data protection rules both exhibit the capabilities of Kardio-Mon and conform to the Wearable Co requirements and preferences.

Policy Management & Enforcement

In the *Policy Management and Enforcement* accountability support service, the Wearable Co does not perform any actions, but they have to receive an account that the machine readable accountability policies are correctly enforced by Kardio-Mon and their third parties. Furthermore, the security expert of the Wearable Co need to be ensured that the access of their clients that want to register to the wearable service is allowed after these clients have given their consent on the provisions of the accountability policies and the action for the acceptance has been logged for any future reference.

Validation

In the *Validation* accountability support service, the data protection officer of the Wearable Co may access the instance of the AAS tool, developed in A4Cloud, which is deployed within Kardio-Mon and request to audit the data handling procedures of Kardio-Mon. The tool can subsequently be used by the Wearable Co to define certain audit tasks and realise the compliance of the Kardio-Mon practices to the agreed accountability policies.

Apart from performing audits to Kardio-Mon, the Wearable must be able to demonstrate their compliance to their legal and social obligations to any cloud auditor or supervisory authority. As such, and since the Wearable Co do not maintain any ICT resources, the AAS instance of Kardio-Mon may be used as source of evidence information for the performance of these audits.

Incident Management

In the *Incident Management* accountability support service, the data protection officer of the Wearable Co must be able to handle upon the detection of any incidents in the cloud environment referring to their business. As such, A4Cloud offers IMT, which is used as the dashboard for the Wearable Co to receive alerts and notifications from Kardio-Mon about any incident, like data breach or policy violation, detected along the provision of the wearable service from Kardio-Mon, including their third party agreements with Map-on-Web and DataSpacer. For this use case, and due to the nature of the Wearable Co, IMT is deployed and offered by Kardio-Mon. Through this tool, the data protection or security expert of the Wearable Co can make decisions on the appropriate management procedures to handle the incidents.

Notification

In the *Notification* accountability support service, the Wearable Co accepts the responsibility for informing their clients on any incidents that should be reported to them, according to the regulations and the agreed accountability policies. In this case, the Wearable Co makes use of the IMT instance of Kardio-Mon and initiates the notification process. The result of this process is the production of client specific notification reports that should be communicated from Kardio-Mon (as the ICT technology provider of the Wearable Co) to the Wearable Co clients on behalf of the Wearable Co.

Remediation

In the *Remediation* accountability support service, the Wearable Co may decide on how to respond to the reported incidents through the use of external tools. For the wearables use case, any required tool support for the implementation of this service is left outside of the scope of this deliverable. For the sake of completeness, we state that the expected actions from the Wearable Co perspective include i) the communication with Kardio-Mon, analysing the exposure of the risks related to the incident and requesting the execution of certain security controls (already be implemented in Kardio-Mon or the other cloud providers Map-on-Web and DataSpacer), and ii) the establishment of communication with the Wearable Co clients to support them exercising their rights to claim for actions, in accordance to a defined remediation process.

4.1.2 The perspective of Kardio-Mon

From the analysis presented in Section 3.2.2, Kardio-Mon needs to implement the following accountability support services.

Policy Definition and Validation

In the *Policy Definition and Validation* accountability support service, the main activities that should be performed by Kardio-Mon relate to the development of the machine readable representation of the accountability policies, in collaboration / negotiation with the Wearable Co. The implementation of the use case assumes the following:

- The privacy officer and/or the security expert of Kardio-Mon has already used COAT and DPIAT to respectively select Map-on-Web and DataSpacer through a risk assessment approach.
- A set of accountability policies is already in place governing the operational phase of the wearable service by Kardio-Mon. These policies represent the matching of the capabilities offered by Map-on-Web and the DataSpacer and the respective requirements and/or preferences of Kardio-Mon to run the wearable service.
- The negotiation of the policies with the various cloud actors is handled outside the A4Cloud use case.

In detail, Kardio-Mon analyses the obligations resulting from the acceptance of the responsibility for operating a cloud instance of the wearable service, which collects personal data from various end user devices and processes them in a way that the end users can manage the history of their collected data and get statistics for their health data metrics in time and geographical terms. It, also, examines the previously signed service level agreements with Map-on-Web and DataSpacer, which reflect the capabilities of these providers to offer specific functional, security and privacy services to Kardio-Mon.

A4Cloud supports Kardio-Mon in this accountability service through the DPPT tool. The latter can be used by the privacy officer or the security expert of Kardio-Mon to compile the human readable form of the contract between Kardio-Mon and the Wearable Co to machine readable policies, expressed in the A-PPL policy language specification. In order to do so, Kardio-Mon considers the abstract policy statements, with respect to the capabilities of Map-on-Web and DataSpacer, which are expressed in AAL. At any time of the policy definition process, the Kardio-Mon actor can load the A-PPL policies to AccLab, offered by A4Cloud, and perform a compliance check of the under development A-PPL policies for the Wearable Co with the already activated policies with Map-on-Web and DataSpacer.

The policy definition supported by DPPT results in Kardio-Mon specifying the following in the A-PPL policies (see Annex 9.1.2 for the machine readable accountability policies):

- The list of personal data that the policy refers to (see Annex 9.1.1).
- The access rights for managing (read, update, delete) each of this data from each of the business roles (Wearable Co client, Employee of the Wearable Co, Map-on-Web) defined for the wearable service application;
- The data handling policy, entailing the data retention period, the allowable geographical locations for collection, processing and storage and the purpose of use. In this part, DPPT also allows Kardio-Mon to define the rules for Map-on-Web subject to which this actor downloads personal data on their environment (i.e. their own A-PPLE) for additional processing required by the contract agreement. For simplicity in this use case, we have not considered this part.
- The set of obligations undertaken by Kardio-Mon in order to be accountable to the Wearable Co, which are implemented through their data handling practices. These obligations list a number of actions that Kardio-Mon is responsible for performing, like the information of the Wearable Co customers about collecting and processing, purpose, location, recipients, rights, the notification of a Data Protection Authority (DPA) that personal data is about to be collected, the request for use consent in order for the processing of the data handled from this policy to start, the notification of the customers in cases of various incident types (security breach, policy violation, etc.), the activation of logging mechanisms for policy enforcement, etc.

Policy Management and Enforcement

In the *policy management and enforcement* accountability support service, Kardio-Mon should be able to activate the machine readable policies developed for the instance of the wearable service of the Wearable Co on their environment and the environment of the third party cloud providers. The enforcement of the appropriate A-PPL based policy requires the deployment of the A4Cloud tools instances that will take advantage of the policy rules at the operational level. As such, the activities of Kardio-Mon in this service assume that the Kardio-Mon IT department have deployed:

- A-PPLE to enforce the policy rules for the Wearable Co instance of the wearable service. The communication of the policies to A-PPLE is handled automatically through the interaction of DPPT to A-PPLE, which is an action logged by A-PPLE for compliance reference.
- AAS to enforce the policy rules for monitoring security and privacy attributes on the SaaS level of the wearable service. This instance of AAS needs to be manually fed with the A-PPL policy from the IT operator of the wearable service to allow appropriate configuration.

The communication of the A-PPL policies to Map-on-Web and DataSpacer is performed manually without any tool support from A4Cloud.

In this accountability support service, we, also, include the operational execution of the wearable service from the Wearable Co customers. Any time that the wearable service performs any action on the personal data of the customers, as a result of a user level manual task (i.e. an actor of the web-based application requests for a functionality) or a service level business operation (e.g. the back end wearable service allows the execution of certain programmable interface functionalities), Kardio-Mon has to enforce the A-PPL policy rules.

Monitoring and Environment State Collection

In the *monitoring and environment state collection* accountability support service, Kardio-Mon has to implement the appropriate mechanisms to facilitate the collection of logs generated by the ICT system components, as a result of the runtime operation of the wearable service and the potential abnormal behaviour from external factors (i.e. intrusion attempts, data loss, etc.). As Kardio-Mon operates the wearable service in the SaaS cloud service model, A4Cloud provides to this actor a set of tools that are deployed by Kardio-Mon to serve the monitoring of the Kardio-Mon cloud environment. These tools are:

- A-PPLE, which generates logs with respect to the enforcement of the policy rules and the decisions made by the engine in response to a business operation (i.e. the employee of the Wearable Co requests for accessing the list of the Wearable Co customers) or a data protection requirement (i.e. expiration of the retention period set in the A-PPL policy for storing the personal data of a certain customer).
- AAS, which monitors the events generated in the SaaS protocol stack when operating the wearable service instance for the Wearable Co and collects logs related to potential security breaches or policy violations.

Collection and Management of Evidence

In the *collection and management of evidence* accountability support service, A4Cloud offers Kardio-Mon the AAS tool, which processes the machine-generated logs collected in the previous service and compiles evidence records. Through these records, Kardio-Mon may provide an evidence-based account to any external actor in order to demonstrate their compliance with the applied regulatory framework and the agreed contracts and accountability policies. Through AAS, Kardio-Mon should be able to manage the lifecycle processes for these logs, subject to particular security and logs collection requirements.

The operation of AAS instance of Kardio-Mon in this service is supported by the A4Cloud TL tool. This tool allows Kardio-Mon manage the lifecycle of the collected logs, from their collection phase through the processing and storage phase and potentially up to the disposal phase.

Incident Management

In the *incident management* accountability support service, Kardio-Mon requires the deployment of the A4Cloud IMT tool, which handles the incidents arising from the analysis of the collected logs and their compilation to evidence records. The incidents reaching the Kardio-Mon environment may have been raised from: i) the Map-on-Web environment, as a result of the security and data protection monitoring rules happening in this cloud SaaS provider, ii) the DataSpacer environment, as a result of the security and data protection monitoring rules happening in this cloud IaaS provider, or iii) the Kardio-Mon environment itself, as a result of the monitoring tasks of the Kardio-Mon AAS instance. The machine driven incidents may refer to a potential policy violation or a security breach.

The implementation of this service through IMT is governed by the incident management team of Kardio-Mon. This actor is responsible for accepting an incident received in IMT and operating the process of the IMT tool to make an assessment on the appropriate way to handle the incidents received in this tool

instance. Furthermore, the IMT operator of Kardio-Mon may use this tool for any perceived incidents within Kardio-Mon that have not been detected from any tool. In this case, the implementation of this service foresees the manual registration of incidents into the IMT instance of Kardio-Mon.

Notification

In the *notification* accountability support service, Kardio-Mon should be able to act upon the result of the assessment performed by the IMT operator in the previous service. In that respect, the incident management team of Kardio-Mon is responsible for enacting the implementation of the notification obligations, as they have been expressed in the A-PPL policies agreed between Kardio-Mon and the Wearable Co. The enforcement of notification is attributed to the A-PPLE instance of Kardio-Mon. The respective notification report includes information about the type of the detected incident, its title and description, and the timestamp of the incident occurrence and detection.

Remediation

In the *remediation* accountability support service, the incident management team of Kardio-Mon is responsible for coordinating the execution of the remedies, dictated either by the adopted obligations (i.e. deletion of backups including personal data for which the retention duration has expired) or by the Wearable Co customers, who may take over on which redress actions should be implemented for their data. In this use case, the implementation of the remediation or redress actions on the Kardio-Mon environment is restricted to the deletion request for a customer's data disclosure affected by the reported incident.

Validation

In the *validation* accountability support service, Kardio-Mon delivers the AAS User Interface, which has been implemented in A4Cloud to support this cloud provider to demonstrate their compliance to the performed data handling processes, through evidence. The demonstration may be triggered by internal organisational process or external obligations. In the first case, the business compliance team of Kardio-Mon may use AAS to create audit tasks relevant to the A-PPL policies to conduct periodic assessment of their data handling processes.

As part of their data protection obligations, the business compliance team of Kardio-Mon offer any third party cloud auditor or supervisor authority the ability to conduct external audits on a periodic or a case-by-case basis. The implementation of these audits allows Kardio-Mon to validate (or not) their business compliance level through audit reports, which include the evidence records corresponding to specific audit tasks and any related supporting documents, like the machine-generated logs comprising the records and the machine readable policies that govern the data handling procedures of Kardio-Mon for the specific audit task.

4.1.3 The perspective of Map-on-Web

From the analysis presented in Section 3.2.3, Map-on-Web needs to implement the following accountability support services.

Policy Definition and Validation

In the *Policy Definition and Validation* accountability support service, Map-on-Web would have to implement the A4Cloud tools as done for Kardio-Mon. However, for simplicity reasons, we consider that Map-on-Web does not process any personal data, thus this accountability support service is not relevant for our case. However, in the general case that the filtering of the data collected from the Wearable Co customers were submitted from Kardio-Mon to Map-on-Web, this cloud provider should have followed the practices of Kardio-Mon, as described in Section 4.1.2. More specifically:

- When Map-on-Web needs to select an appropriate SaaS, PaaS or IaaS cloud provider to collaborate in order to deliver the map visualisations of big data streams, the privacy officer of this provider has to use COAT and DPIAT tools. We assume that for the wearables use case in this deliverable the privacy officer of Map-on-Web has already used these tools to select DataSpacer as the storage cloud provider, through a risk assessment approach, which consulted Map-on-Web that a detailed data protection impact assessment is not required.
- Although for our case Map-on-Web does not collect and store any personal data, in the general case that the filtering of the data collected from the Wearable Co customers were submitted from

Kardio-Mon to Map-on-Web, this cloud provider should have used DPPT to define the accountability policies, subject to which the retrieval of this data from Kardio-Mon and their processing from Map-on-Web should have been performed. At this stage, Map-on-Web would have also used AccLab to validate that the suggested policies do not violate the capabilities of DataSpacer. As said, for simplicity reasons, we leave this case outside of the scope of this deliverable.

Policy Management and Enforcement

In the *policy management and enforcement* accountability support service, Map-on-Web should be able to enforce the machine readable policies governing their collaboration with Kardio-Mon, through a dedicated A-PPLE instance deployed from the IT department of Map-on-Web. As no collection and processing of personal data is performed by Map-on-Web in our case, this support service is not relevant here.

Monitoring and Environment State Collection

In the *monitoring and environment state collection* accountability support service, Map-on-Web deploys the appropriate A4Cloud tools for monitoring the communication with Kardio-Mon. The respective tool is AAS, which collects logs with respect to the secure interaction of Map-on-Web and Kardio-Mon in order to receive the streams of statistical data. In that respect, Map-on-Web can verify their compliance to a bilateral contract agreement with Kardio-Mon for a secure communication in order to accomplish the delegated functional tasks.

Collection and Management of Evidence

In the *collection and management of evidence* accountability support service, Map-on-Web exploits the AAS tool to process the machine-generated logs collected in the previous service and compile the corresponding evidence records. The latter are maintained internally in the Map-on-Web to provide an evidence-based account to Kardio-Mon or any other external actor, upon a request for demonstrating the compliance of this cloud provider with the established contract. As in the case of Kardio-Mon, Map-on-Web should be able to use AAS to manage the lifecycle processes for the collected logs, subject to particular security and logs collection requirements. As a secure evidence storage, the AAS instance of Map-on-Web uses the A4Cloud TL tool.

Incident Management

In the *incident management* accountability support service, Map-on-Web should deploy IMT to handle the incidents arising from the analysis of the collected logs and their compilation to evidence records. In the general case that Map-on-Web would process and store personal data from the Wearable Co customers, this IMT instance of Map-on-Web should be configured to receive incidents from: i) the DataSpacer environment, as a result of the security and data protection monitoring rules happening in this cloud IaaS provider, or ii) the Map-on-Web environment itself, as a result of the monitoring tasks of the Map-on-Web AAS instance. In that case, the IMT operator of Map-on-Web would be responsible for accepting an incident received in IMT and operating the process of the IMT tool to make the necessary user assessment on how to address the incidents received in this tool instance. Furthermore, the IMT operator of Map-on-Web could use this tool for any perceived incidents within Map-on-Web that have not been detected from AAS. Due to simplicity, the actual environment of the final A4Cloud use case prototype does not consider any IMT instance for Map-on-Web.

Notification

Following the previous service, in the *notification* accountability support service, Map-on-Web should be able to act upon the result of the assessment performed by the IMT operator for a received or perceived incident. As Map-on-Web is a cloud processor in our wearables use case, this IMT instance functions only for the case that Map-on-Web needs to notify Kardio-Mon for any incident referring to an insecure data communication between these two providers.

Remediation

As happens for Kardio-Mon, in the *remediation* accountability support service, the incident management team of Map-on-Web would be responsible for coordinating the execution of the remedies, dictated either by the adopted obligations (i.e. deletion of backups including personal data for which the retention duration has expired) or by Kardio-Mon, who should be able to request for the implementation on certain

redress actions. For this deliverable and the wearables use case, this accountability support service is not considered.

Validation

In the *validation* accountability support service, Map-on-Web allows access to the User Interface of their AAS instance. Through this A4Cloud tool, Map-on-Web may allow internal or external audits, as explained for Kardio-Mon in section 4.1.2.

4.1.4 The perspective of DataSpacer

From the analysis presented in Section 3.2.4, DataSpacer needs to implement the following accountability support services.

Policy Definition and Validation

In the *Policy Definition and Validation* accountability support service, the main activities that should be performed by DataSpacer relate to the specification of accountability policies, detailing how this cloud IaaS provider should process and store personal data of the Wearable Co customers on behalf of Kardio-Mon. As explained in Section 3.2.4, the relevant lifecycle phase precedes the conceptualisation of the wearables use case application by the Wearable Co, thus this accountability support service is not relevant for our case. This means that before that phase the privacy officer and/or the security expert of DataSpacer should have used DPPT to define an accountability policy for Kardio-Mon, with respect to the allowable geographical locations and data transfers of the storage area for the wearable service instance of the Wearable Co.

We can, also, refer to the following examples that DataSpacer could make use of the A4Cloud tools implementing this accountability support service in a potential extension of the scenario:

- Use of multi clouds for storage purposes: we assume that DataSpacer needs to identify an appropriate collaborating IaaS cloud provider in case that the management board of DataSpacer decides to work on a scenario for operating backups of their customers' business in a third party storage provider. In such a case, the privacy officer and/or the security expert of DataSpacer should use COAT and DPIAT, respectively.
- Support for data processing: we assume that DataSpacer offers additional cloud services than simple storage of the personal data of the Wearable Co customer provided by Kardio-Mon. In such a case, the privacy officer and/or the security expert of DataSpacer should use DPPT to specify the provisions of the accountability policies that would govern the data handling procedures of DataSpacer.
- Provide personal data storage facilities to Map-on-Web: in such a case, Map-on-Web would require to agree with DataSpacer on the allowable data transfers for the personal data of the Wearable Co customers. This agreement would consider the enforcement of the policy agreed between Kardio-Mon and DataSpacer about the personal data collected and processed in the context of the wearable service instance for the Wearable Co. In other words, the allowable data transfers agreed between Map-on-Web and DataSpacer should be a subset of the ones agreed between Kardio-Mon and DataSpacer.

Policy Management and Enforcement

In the *policy management and enforcement* accountability support service, DataSpacer must deploy DTMT and configure it, so that the accountability policy specifying the allowable data transfers in the wearables use case are enforced at the operational level. The result from the implementation of this service for DataSpacer is a policy checking action on the events happening on the networking layer of this IaaS cloud provider.

In the extended scenario for supporting further data processing service presented above, this accountability support service would be relevant, in the sense that DataSpacer should deploy an A-PPLE instance to enforce the policy agreed with Kardio-Mon.

Monitoring and Environment State Collection

In the *monitoring and environment state collection* accountability support service, DataSpacer needs to deploy an AAS instance as well, which is configured with the policies for the allowable data transfers.

Subsequently, both DTMT and AAS are used by the IT operators of DataSpacer to monitor the execution of the wearable service. Through these tools, DataSpacer is able to collect logs generated by the ICT system components, as a result of the runtime operation of the wearable service and the potential abnormal behaviour from external factors (i.e. intrusion attempts, data loss, etc.). Due to the cloud service operating model of DataSpacer, this provider can use DTMT to monitor the interactions happening on the network layer of the IaaS protocol stack and exploit AAS to monitor the events generated by the cloud infrastructure along the operation of the wearable service instance for the Wearable Co, which may relate to an abnormal behaviour of the DataSpacer environment.

Collection and Management of Evidence

In the *collection and management of evidence* accountability support service, DataSpacer uses the AAS tool, which processes the machine-generated logs collected in the previous service and compiles evidence records. Through these records, DataSpacer may provide an evidence-based account to any external actor in order to demonstrate their compliance with the applied legal framework and the agreed contracts and accountability policies with Kardio-Mon. Through AAS, DataSpacer should be able to manage the lifecycle processes for these logs, subject to particular security and logs collection requirements.

The operation of AAS instance of DataSpacer is this service is supported by the A4Cloud TL tool. This tool allows DataSpacer manage the lifecycle of the collected logs, from their collection phase through the processing and storage phase and potentially up to the disposal phase.

Incident Management

In the *incident management* accountability support service, DataSpacer requires the deployment of an IMT instance, which handles the incidents arising from the analysis of the collected logs and their compilation to evidence records. The incidents reaching the IMT instance of DataSpacer have been raised from the DataSpacer environment itself, as a result of the security and data protection monitoring rules happening on the IaaS layer of this provider, or the monitoring tasks of the AAS instance of DataSpacer. The machine driven incidents may refer to a potential policy violation with respect to the allowable locations or a security breach.

The implementation of this service through IMT is governed by the incident management team of DataSpacer. This actor is responsible for accepting an incident received in this IMT instance and operating the process of the IMT tool to make an assessment on how this incident should be addressed. Furthermore, the IMT operator of DataSpacer may use this tool for any perceived incidents within the DataSpacer environment that have not been detected from either DTMT or AAS. In this case, the implementation of this service foresees the manual registration of incidents into the IMT instance of DataSpacer.

Notification

Subject to the user assessment for the criticality of the incidents in the previous service, in the *notification* accountability support service, DataSpacer should be able to act upon this assessment. More specifically, the IMT operator of DataSpacer must be responsible for enacting the implementation of the notification obligations, as they have been expressed in the A-PPL policies agreed between Kardio-Mon and DataSpacer. The notification process includes the production of the relevant notification report, which is communicated to Kardio-Mon through a machine-to-machine interaction between the IMT instances of these two cloud providers.

Remediation

In the *remediation* accountability support service, the incident management team of DataSpacer is responsible for coordinating the execution of the remedies, dictated either by the adopted obligations (i.e. reverting actions resulting to data transfers violating the agreement with Kardio-Mon) or by Kardio-Mon, who may take over on which redress actions should be implemented from DataSpacer. In this use case, the implementation of the remediation or redress actions on the DataSpacer environment is restricted to ensuring that, after a notification is reported, the storage of the personal data stored from the wearable service to DataSpacer is happening only in accordance with the allowable data transfer policy rules.

Validation

In the *validation* accountability support service, DataSpacer allows access to the User Interface of their AAS instance. Through this A4Cloud tool, DataSpacer may allow internal or external audits, as explained for the case of Kardio-Mon in section 4.1.2.

4.1.5 The perspective of the Wearable Co Customer

As explained in Section 3.2.5, the Wearable Co Customer does not implement any accountability support services, but is the consumer of the actions happening when the other cloud actors of the wearables use case implement these services. Thus:

- During the implementation of the *Policy Definition and Validation* accountability support service from the Wearable Co and Kardio-Mon, Kardio-Mon may use DPPT to specify an instance of the policy agreed with the Wearable Co that complies with the preferences of the Wearable Co customer for certain data protection requirements. As we do not support in this use case, any policy negotiation, this implementation step has not been considered here.
- During the implementation of the *policy management and enforcement* accountability support service from Kardio-Mon, the Wearable Co customers must give their consent for the collection and processing of their personal data. This is a policy enforcement point for Kardio-Mon that is addressed in this service.
- During the implementation of the *notification* accountability support service from Kardio-Mon, the Wearable Co customers must be able to access the notification reports directed to them. This is achieved through the deployment of the RRT tool provided by A4Cloud in the end user device of the Wearable Co customer.
- Following the communication of a notification report, in the *remediation* accountability support service, the Wearable Co customer is equipped with RRT to access remediation and redress suggestions, subject to the nature of the received notification. This tool enables the Wearable Co customers exercise their right for controlling how their data is handled by Kardio-Mon (and the third party providers DataSpacer and Map-on-Web).
- During the *validation* accountability support service, the Wearable Co customer is equipped with DT, which supports them exercising their right for requesting transparency from Kardio-Mon on how this actor implements the agreed data handling procedures. Through DT, the customers can access their data disclosures in the context of operating the wearable application (and the back end wearable cloud service).
- The Wearable Co customer may, also, activate the *validation* accountability support service by informing the respective Data Protection Authority for a perceived or reported incident and requesting an audit on the Kardio-Mon data handling procedures.

It must be noted that during the involvement of the Wearable Co customer in the notification, remediation and validation accountability support services, the communication of the customer with Kardio-Mon is supported by TL, which offers a secure and encrypted channel for bridging the customer with the cloud environment.

4.2 The physical deployment of the wearables use case components

In this section, we provide the presentation of the physical deployment of the A4Cloud tools instantiation and the respective applications for the wearables use case prototype. The tool deployment refers to those A4Cloud tools that has a runtime instance, namely A-PPLE, DTMT, AAS, IMT and TL. The remaining of the tools are mainly facilitating design time functionalities for the setup of the policies.

In Deliverable D47.1, we explained how the deployment environment for this use case has been progressively built and which tools have to be deployed by each cloud provider to support accountability. In this deliverable and in this section, make a summary of that setup and we provide information about the additional tool deployment. Also, we must note that for simplicity reasons, we do not consider all the tool instances expected as per the guidance in Section 2.

DataSpacer is the IaaS cloud provider, which deploys the cloud infrastructure. As we have already explained, the physical deployment consists of an OpenStack installation and for the project purposes it is being hosted at ATC premises. This installation uses the ninth release of OpenStack, called

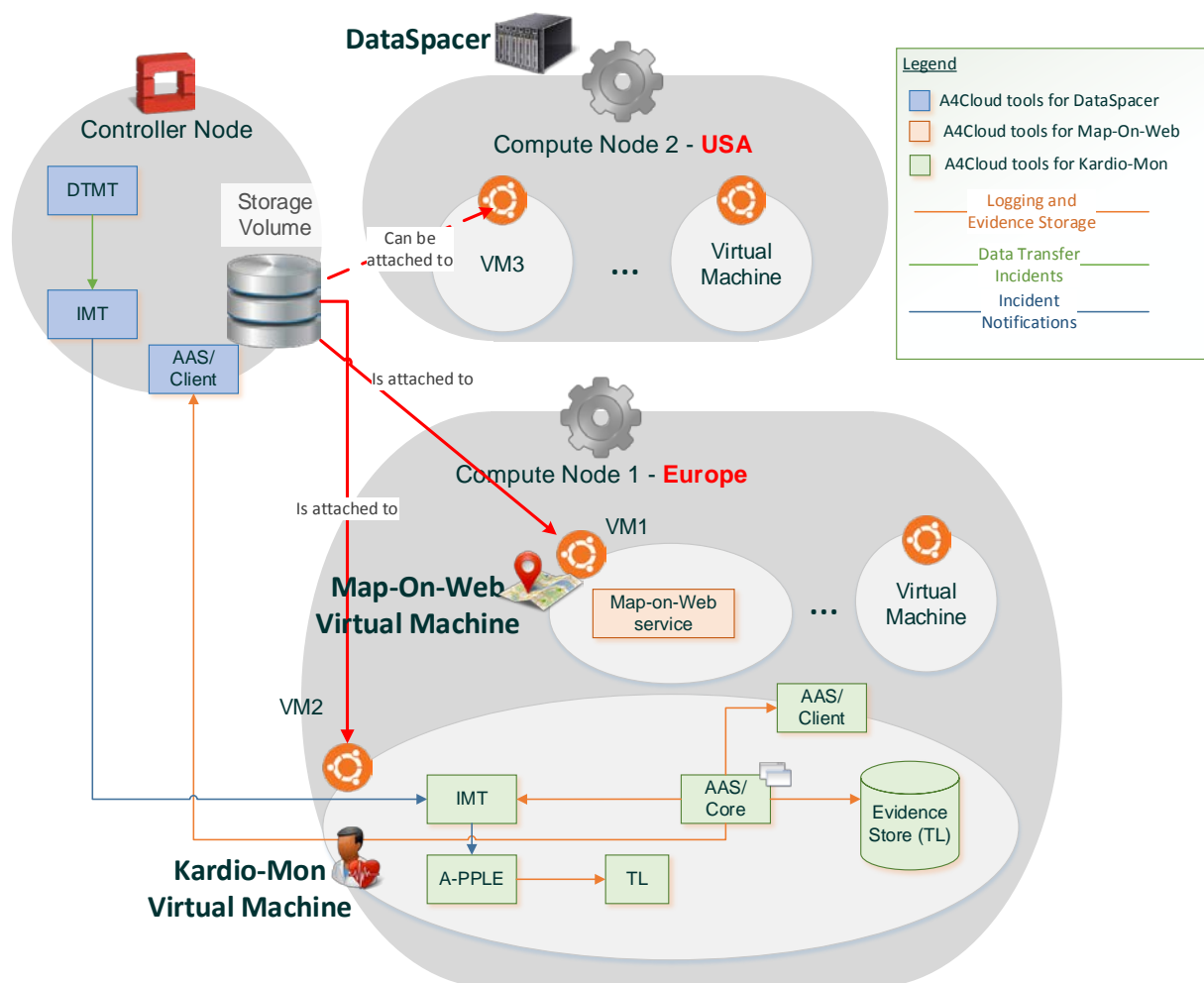


Figure 15: The physical deployment of the A4Cloud tools for the complete cloud service supply chain of the wearables use case

The overall deployment environment is shown in Figure 15. From an accountability perspective, this deployment is important. For that reason, we emphasise on the DataSpacer architecture and the role of the Controller Node and the two Compute Nodes. In this architecture, the responsible IT administrator of DataSpacer deploys the relevant A4Cloud tools, namely DTMT and IMT. More specifically, the Controller Node hosts DTMT to collect logs about data transfers happening within the DataSpacer environment, as they are captured in this node. DTMT embeds a TL instance, which is used to log any actions related to data transfers. Furthermore, IMT is deployed to allow the incident management and response team of DataSpacer to manage the incidents raised within this provider environment.

Based on this infrastructure deployment, DataSpacer allocates cloud resources to Map-on-Web and Kardio-Mon to host their SaaS offerings and provide cloud services to their potential customers. In the wearables use case, we assume that both Map-on-Web and Kardio-Mon select to use the data centres in EEA. So, DataSpacer allocates the requested resources from Compute Node 1 in the form of VMs. Both Virtual Machine 1 and Virtual Machine 2, which host the Map-on-Web and the Kardio-Mon services respectively, are running a 64 bit Ubuntu Operating System version 14.04.

Within each VM (1 and 2), the relevant SaaS cloud providers deploy their own accountability tools. For our case and in order to simplify the use case prototype environment, we consider that VM 1 hosting Map-on-Web does not maintain any personal data and A4Cloud tools, but it only hosts the Map-on-Web cloud service implementation.

In turn, Kardio-Mon reserves its own cloud resources through a dedicated VM in Compute Node 1 of DataSpacer and deploys the respective A4Cloud tools. Figure 15 demonstrates the deployment of the cloud environment and the A4Cloud tools for the wearables use case. As it can be seen there, Kardio-Mon creates its own instances of the A4Cloud tools, thus:

- The TL instance connected to the A-PPLE instance, which is used for the encrypted storage of the logs created by this A-PPLE instance (logs related to the access and usage of PII, following the underlying policy rules) and in order to serve the communication of A-PPLE with the tools hosted in the devices of the Wearable Co customer.
- The A-PPLE instance, which is used to enforce the accountability policies.
- The AAS core and clients, which are used to collect the logs from the various tools and the protocol stack and transform them to evidence records, before they are maintained in the Evidence Store instance.
- The IMT instance to allow the incident management and response team of Kardio-Mon to handle the incidents raised within this VM-2 or perceived by Kardio-Mon itself.

Using these tools, the different cloud providers are able to implement the accountability support services.

4.3 The use of A4Cloud tools in the implementation of the wearables use case

Following the instantiation of the reference architecture from the perspective of the cloud actors involved in the wearables use case, in this section we summarise the use of the A4Cloud tools and the consumption of the respective accountability artefacts during the implementation of the accountability support services by each role. These services allow the actors to run the processes of the lifecycle for accountability, in order to be accountable to their collaborating business actors. Furthermore, in this section we present the physical deployment of the final use case prototype. It must be noted that the contents of this section exploit the descriptions provided in Section 2.3 for the guidance on the adoption of the Accountability Framework and the implementation of the accountability support services.

Table 3: Mapping the wearables use case actors to the business actors of the reference environment (Figure 1)

Wearables use case actor	Business actor of the reference cloud environment
Wearable Co Customer	Client
Wearable Co	Cloud Customer
Kardio-Mon	Primary CSP
Map-on-Web	SaaS CSP
DataSpacer	IaaS CSP
Cloud Auditor	Cloud Auditor

Table 3 presents the mapping of the actors between the wearables use case and the reference cloud environment of Figure 1. This table is used as reference for the reader in order to explain the instantiation of figures in Section 2.3 for the use case actors in the wearable service.

4.3.1 Policy Definition and Validation

In this section we elaborate on the involvement of the use case actors in the policy definition and validation accountability support process. Following the interactions shown in Figure 3, the relevant cloud providers, Kardio-Mon, Map-on-Web and DataSpacer allow COAT to retrieve their capabilities in terms of the Service Level Agreements (SLAs) they offer, their certificates and the contracts that provide to their customers, including the list of other third party providers they collaborate. Through this information, COAT can build the cloud service offering of each provider.

When the privacy expert of the Wearable Co wants to select a cloud provider, they invoke the COAT tool, which is Web-based and it can be accessed from a Web browser. This tool guides the privacy expert to provide their requirements for selecting a provider, based on the functional, security and privacy needs. In order for the Wearable Co officer to run COAT, they have to have investigated on their obligations resulting from the legal and social norms, which are applicable for the wearables use case application that the Wearable Co wants to operate.

COAT offers the privacy expert of the Wearable Co a list of cloud service offers that match their requirements. Through a continuous dialogue for the investigation of the Wearable Co requirements, the privacy expert is finally able to select a cloud provider for providing the wearable service, which is Kardio-Mon.

The next step for the privacy expert of the Wearable Co is to perform a data protection impact assessment process, regarding their decision to run their business for the management of the data collected from the wearable devices they sell to their Wearable Co customers on the cloud, using the cloud service offered by Kardio-Mon. Thus, they invoke the DPIAT tool, which is Web-based and it can be accessed from a Web browser. As shown in Figure 3, DPIAT initially offers the pre-screening questionnaire, which is a pre-assessment test for the privacy expert of the Wearable Co to be aware of whether they need to run a data protection impact assessment process. If so, DPIAT loads a set of 50 questions, asking the expert on the wearables use case project, the collection and usage of the information coming from the wearable devices, their storage and security requirements, the restrictions on transferring information to third parties and other cloud specific questions. Through this approach, DPIAT educates the privacy expert of the Wearable Co about the risks arising from their decisions and how they can reduce these risks by selecting Kardio-Mon or any other cloud provider. Through this process, the privacy expert can assess the risks of running the wearables use case application in the cloud, from a data protection perspective.

The next step in this accountability support service is to define the policies. To this end, the Wearable Co communicates Kardio-Mon their willingness to establish an agreement with them to run their wearable application through an instance of the Kardio-Mon wearable service. This offline process includes the submission of their requirements on how this instance should be instantiated for their case in order to address the particular functional, security and privacy requirements. Kardio-Mon on their end negotiates a set of policies with the Wearable Co. Thus, the privacy officer of Kardio-Mon uses DPPT in order to compile a lawyer readable privacy policy into a machine readable policy representation, as shown in Figure 4. This will be the proposal of Kardio-Mon to the Wearable Co for the set of policy rules that should be enforced to operate the wearables use case application.

The privacy expert of the Wearable Co can validate the accuracy and compliance of the machine readable policy through AccLab (see Figure 4). In order to support this, we have assumed that the privacy officer of Kardio-Mon has used AccLab to create a list of abstract policy statements in AAL, representing their capabilities. This list is communicated to privacy expert of the Wearable Co and be used for performing compliance checks between the machine readable policy and the AAL statements. The Wearable co can also use AccLab to find the desirable policy, matching their preferences expressed in the same form as the Kardio-Mon capabilities (in AAL).

Finally, as shown in Figure 4, there might be an optional negotiation phase between the privacy expert of the Wearable Co and the privacy officer of Kardio-Mon, so that we conclude on the exact policy match. The last step is for privacy officer of Kardio-Mon to submit the agreed A-PPL policy to the A-PPLE instance of Kardio-Mon.

4.3.2 Policy Management and Enforcement

In this accountability support service, we take advantage of the deployment description in Section 4.2 and we describe the actions taken by the wearables use case actors to enforce the agreed policies in the cloud environment. Thus, following the interactions shown in Figure 5, in this accountability support service, Kardio-Mon uses DPPT to load the agreed A-PPL policy into their A-PPLE instance and configure the AAS instance of Kardio-Mon with this policy rules. In addition to it, Kardio-Mon configures the IMT instance to register the Wearable Co service business as subscriber of the notifications (through the end point of the Kardio-Mon A-PPLE instance).

Furthermore, Kardio-Mon requests the configuration of the A4Cloud tools in DataSpacer as well (since, as we explained in Section 4.2, Map-on-Web does not maintain any accountability tools). To this end, DataSpacer configures DTMT to raise incidents on potential data transfer violations for the resources allocated to Kardio-Mon, while the IMT instance of DataSpacer is configured so that the IMT instance of Kardio-Mon is registered as a subscriber.

Finally, in this phase, the wearable service application is developed, based on the requirements of the Wearable Co. During the implementation of this application, we consider that the handling of data gathering and processing goes from the application itself to the A-PPLE instance of Kardio-Mon, while the registration to the application is occurred, once a Web page with the rules of the policy offered to the Wearable Co customers is viewed and the customers has given consent to the provisions of the policy.

4.3.3 Monitoring and Environment State Collection

In the wearables use case, the tools that contribute to the implementation of the monitoring and environment state collection accountability support service are:

- In Kardio-Mon: A-PPLE monitors the enforcement of the A-PPL policy every time that the tool is triggered by the wearable service. AAS deploys a client in the cloud environment to monitor the events generated in the cloud service layer protocol stack and a second client to monitor the events generated in the cloud infrastructure layer protocol stack.
- In DataSpacer: DTMT monitors the networking layer of the cloud infrastructure and the events relating to data transfers between different network virtual nodes.

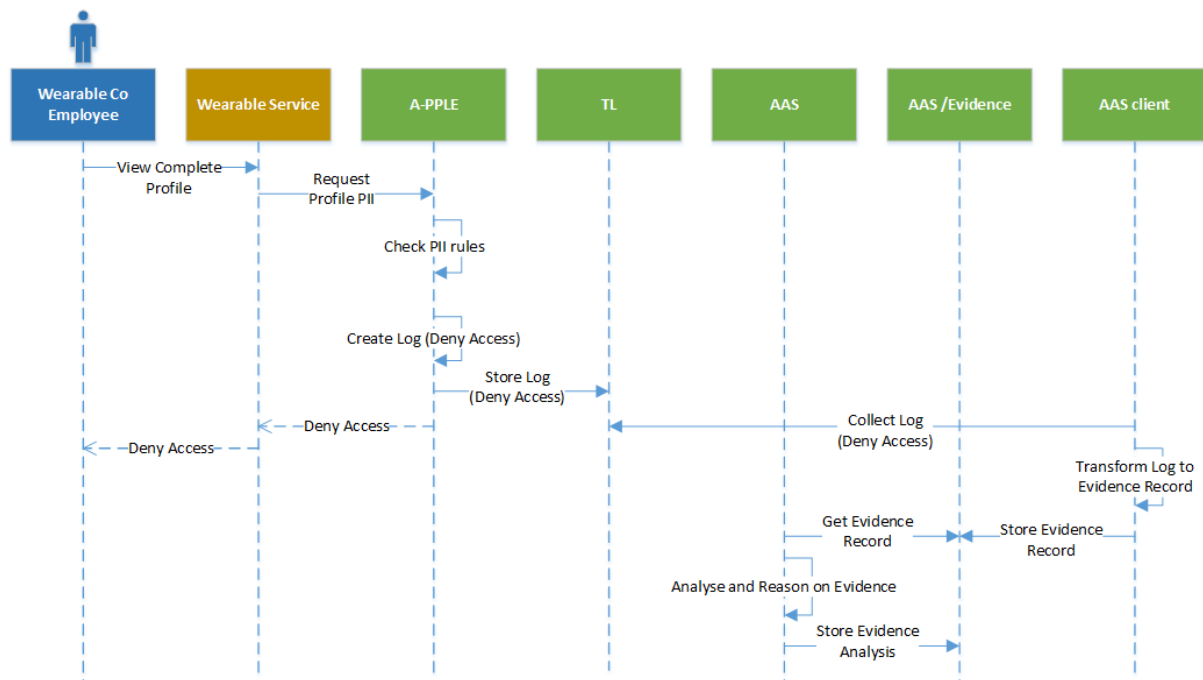


Figure 16: Monitoring and environment state collection – an example from the wearables use case.

In Figure 16, we consider an example of monitoring the environment for a policy enforcement case for an unauthorised access to personal data of the Wearable Co customers. An employee of the Wearable Co accesses the wearable service application and requests to access the personal data of a specific customer. The request for accessing personal data is attributed to the A-PPLE instance of Kardio-Mon, which denies granting access to this request, according to the policy. A-PPLE generates log entries for this action, which are finally collected by the relevant AAS instance. This flow includes processes that also refer to the next accountability support service for the collection and management of evidence.

4.3.4 Collection and Management of Evidence

In this accountability support service, the different business actors in the wearables use case translate the collected logs to evidence. For simplicity reasons, we emphasise only to the case of Kardio-Mon, which deploys an AAS instance, but one of the AAS clients monitors the networking layer as well. Thus, as shown in Figure 7, all the events happening in the service and infrastructure layer of the environment are centrally collected for Kardio-Mon in the core AAS instance, which maintains the Evidence Store (the latter is an implementation of TL for secure storage purposes).

4.3.5 Incident Management

For this accountability support service, we consider that incidents can be raised by:

- DTMT instance of DataSpacer, which automatically provides alerts of potential data transfer policy violations.
- IMT instance of DataSpacer, which allows the respective DataSpacer team to register a perceived incident.
- AAS instance of Kardio-Mon, which automatically reasons on the collected evidence and produces alerts on policy violations or security breaches.
- IMT instance of Kardio-Mon, which allows the respective Kardio-Mon team to register a perceived incident.

An example of the implementation of this service for the wearables use case is shown in Figure 17, which extends the interactions happening in Figure 8.

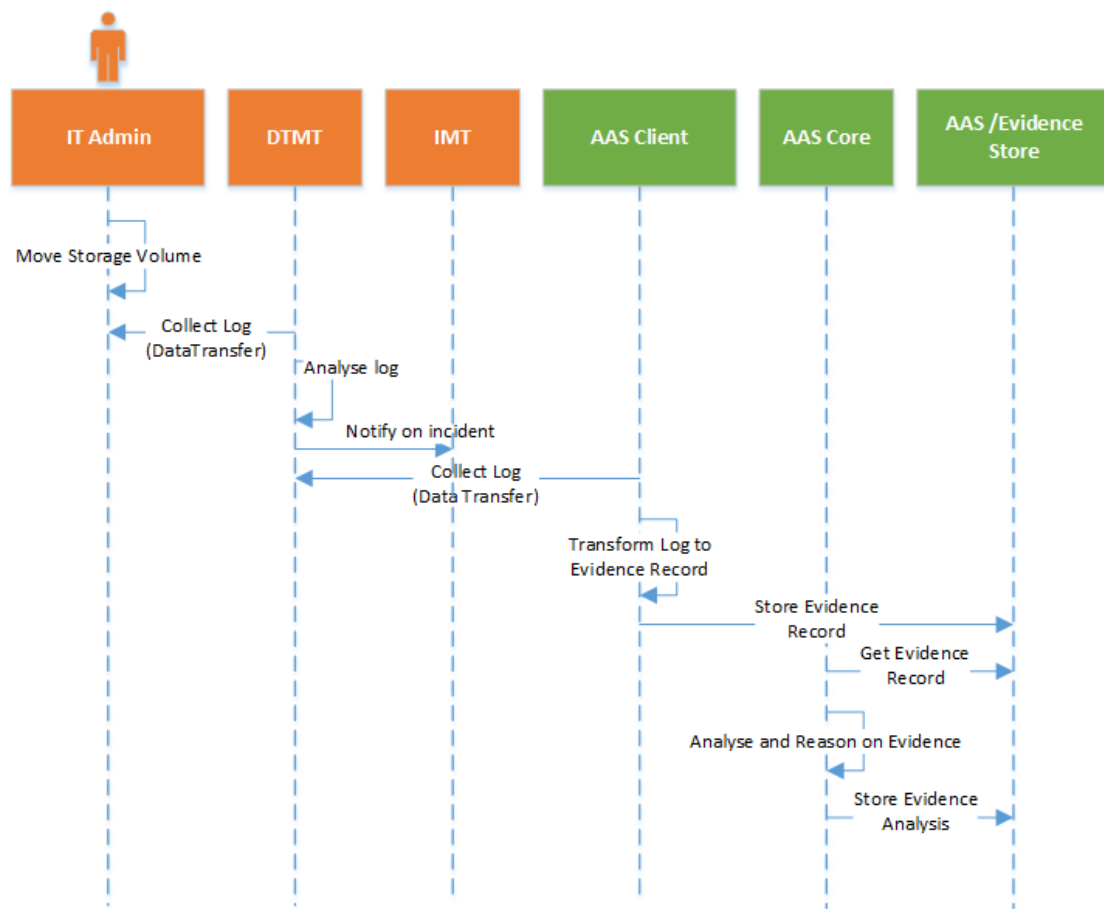


Figure 17: Incident management – an example from the wearables use case.

4.3.6 Notification

In the notification accountability support service, we consider the involvement of the DataSpacer and Kardio-Mon, who are deploying the necessary A4Cloud tools to raise and manage incidents. Considering the example of Figure 17 about a potential data transfer policy violation, we assume that the incident management team of DataSpacer decides that the raised incident is of such a severity and type that it should be communicated, based on the obligations on DataSpacer, to Kardio-Mon. Figure 18 demonstrates the interactions between the actors of the wearables use case to implement the notification service for this data transfer incident.

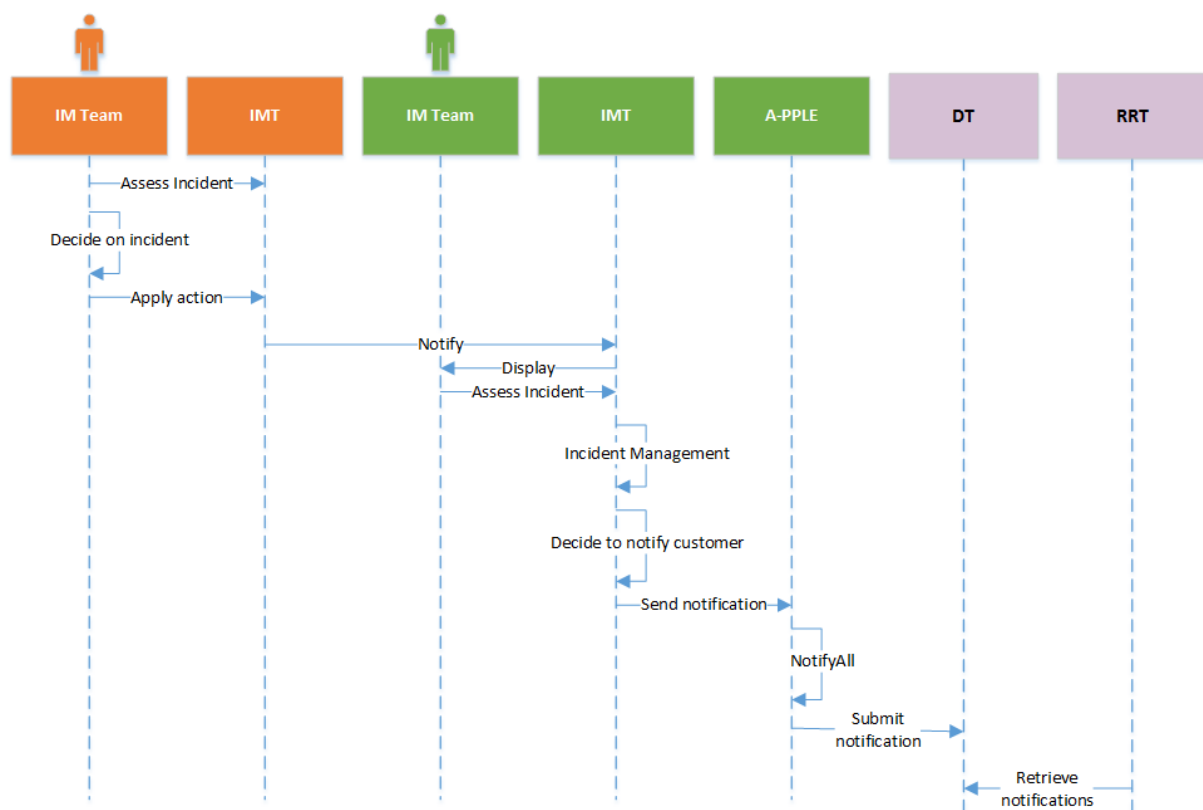


Figure 18: Notification – an example from the wearables use case.

As it can be seen from this figure, the decisions made across the various incident response teams may result this incident to reach the device of the Wearable Co customers, who can handle it through DT and RRT tools.

4.3.7 Remediation

In the wearables use case, the remediation accountability support service is mainly considered for the Wearable Co customers, based on the interactions shown in Figure 11. More specifically, the customers access their DT instance and are notified of received alerts pending their management. By opening the RRT view, they can browse the notifications alerts and for each of them to have a list of remediation actions.

4.3.8 Validation

For the wearables use case, the validation accountability support service is implemented through the AAS instance of Kardio-Mon, which offers a visualisation of the tasks for auditing the way that Kardio-Mon handles the development of the service components for the wearables accountability policy. The respective AAS tool offers the same UI for both the Wearable CO privacy expert and the Cloud Auditor to perform audits on the practices followed by Kardio-Mon. Since in the wearable use case we have an AAS client of the Kardio-Mon instance on the networking part of DataSpacer, the audit tasks may also refer to infrastructure handling processes, like the creation of storage backups and the movement of storage volumes from one compute node to another.

Furthermore, the validation accountability support service is implemented in the final A4Cloud use case prototype by allowing the Wearable Co customers in using DT and access their disclosures with Kardio-Mon and other cloud service providers as well. For demonstration purposes, we have simulated a set of personal data for different fictitious cloud providers, which complement the actual disclosures occurred between the customers and the service offered by Kardio-Mon.

4.4 Concluding the implementation of the use case prototype

In this section, we presented the instantiation on the Cloud Accountability Reference Architecture for the wearables use case. The section tried to emphasise on the updates on the implementation effort since the delivery of the first use case prototype in May 2015 (Deliverable D47.1). The implementation of the application layer components has not changed and the flow of the business information and the functionalities as those already explained in D47.1. The main differences lay on the interface of this use case with the A4Cloud tools for the adoption of the lifecycle of accountability from all the business actors of the wearables use case.

Building on this section, Section 0, presents the scenarios for the demonstration of this use case.

5 Demonstration of the wearables use case

5.1 Introducing the demonstration scenario

This section introduces the scenario selected to demonstrate the capabilities of the final A4Cloud use case instantiation to support accountability, when the personal data of the Wearable Co customers are collected and processed in the wearable service, which is operated by Kardio-Mon, with the involvement of Map-on-Web and DataSpacer.

In order to set boundaries to the demonstration scenario, we first introduce the assumptions that have been made for the presentation of the scenario. These assumptions refer to the time period that the scenario starts, given the real life considerations for such a cloud business, and the steps that must have been executed prior to this start time for all the involved actors in the wearables use case.

5.1.1 The history of the scenario

As we have already presented in D47.1, the cloud providers involved in the wearables use case are established in various time scales, which comprise a chronological order of prerequisite events, so that we are able to demonstrate accountability through the scenario defined in this section. The starting point for our demonstration is the plan of the Wearable Co to offer their clients the ability to manage their personal data, collected from the devices purchased from the Wearable Co, through a Web application. This plan is effective since January 2016. Before this time threshold, we assume that the cloud providers has started their business, as follows.

DataSpacer has started operating as an independent international IaaS cloud provider in 2013, legally established in France. This provider offers cloud storage and computation services out of a number of datacentres located in different geographical locations globally, which are subject to different regulatory frameworks, based on their location. The capabilities of DataSpacer for storing data span across different types of data, for which certain security and privacy requirements are applied. In order for DataSpacer to be accountable to their customers, they have deployed in their environment the A4Cloud tools DTMT, IMT and AAS (integrated with TL for storing logs in a secure way), which are exploited by this provider to develop an accountable way for handling the types of data attributed to their storage and processing facilities. Furthermore, DataSpacer is able to provide an account to their customers on their data handling processes or to any third party cloud auditors and relevant authorities in cases an audit is required, due to a data protection incident.

Six months later, Map-on-Web starts its cloud business in Germany as a SaaS provider to offer data aggregation and visualisation technologies for big data streams. The aggregation process allows the categorisation of the data streams, according to a specific criterion, in order to calculate specific statistical metrics, like their mean values on a given timescale. The visualisation process includes the geographical representation of the data, which is offered as an API for intuitive visualisation to be ported in cloud applications. Both processes require Map-on-Web having access the storage area of the data streams, while temporary storage for the results of their processing might be required. In that respect, and in order for Map-on-Web to be accountable to their customers, they implement the accountability support services, which results in the selection of DataSpacer as their infrastructure cloud provider and the deployment of instances for the A4Cloud tools A-PPLE, AAS, TL and IMT.

Beginning of 2015, Kardio-Mon, a Greek SME, decides to start a cloud business for providing the wearable service, which intends to support the collection of data from wearable devices. This is the case of processing personal data, which means that Kardio-Mon needs to comply with the applied regulatory framework in order to implement the necessary security, privacy and data protection measures so that the company is accountable to their customers. Due to the Kardio-Mon functional, security and privacy needs and obligations as a candidate cloud provider handling personal data, the results for the implementation of the accountability support services for Kardio-Mon are summarised in the following:

- The Kardio-Mon privacy officer uses COAT and DPIAT to select Map-on-Web as the provider to offer data aggregation and visualisation services for the processing of the personal data collected from the wearable devices.
- The Kardio-Mon privacy officer uses COAT and DPIAT to select DataSpacer as the cloud hosting provider.

- The Kardio-Mon IT group implement the wearable service within the DataSpacer resources (the Kardio-Mon virtual machine VM) and deploy A-PPLE for storing personal data and enforcing the accountability policies that will be agreed by the Kardio-Mon customers on a case by case basis.
- The Kardio-Mon IT group deploy AAS (including TL) in the Kardio-Mon VM to monitor the operation of the wearable service and collect logs from the cloud environment for a specific operational stream of the wearable service (for a specific customer). This tool will be used for auditing purposes as well.
- The Kardio-Mon IT group deploy IMT in the Kardio-Mon VM to be able to handle incidents. This IMT instance is configured so that it receives incidents from the IMT instances of Map-on-Web and DataSpacer. These instances are, subsequently configured to include Kardio-Mon IMT instance in their subscribers' list.

Now the Kardio-Mon operated wearable service is ready for the operational phase, which is triggered by having customers offering the network of their wearable devices as sources of the data collection process. This is the case of the Wearable Co, the SME manufacturing wearable devices, which may use a third party cloud service for managing the wearable data and add value to it. These devices are to be purchased by the Wearable Co customers, who will then be able to access and use the third party cloud service to manage their data collected from their wearable device.



Figure 19: An overview of the actors in the wearables use case demonstration scenarios

Figure 19 makes an overview of the business actors that are involved in the demonstration of the scenarios for the wearables use case.

5.1.2 The demonstration scenarios

As we have explained since deliverable D47.1, the complexity of the demonstration process exponentially grows up with the number of interactions considered in the end-to-end approach. As a compromise to present a comprehensive demonstration, we have set boundaries in the presentation of the whole story from the development of the cloud service supply chain to the operational phase of the wearable service. In that respect, we have decided to demonstrate the use case, examining the timeline of the actions happen at the time that the Wearable Co decides to advance their wearable business by offering a cloud service to manage the data collected from the wearable devices.

Given this starting point, our aim is to demonstrate the final prototype of the A4Cloud use case implementation from the perspective of the cloud actors and emphasise on the tool usage for the different phases of the wearables use case implementation. Figure 20 introduces the demonstration scenarios, the involvement of the main business actors, according to their cloud and data protection role in the wearables use case, and the use of the A4Cloud tools to accomplish these scenarios.

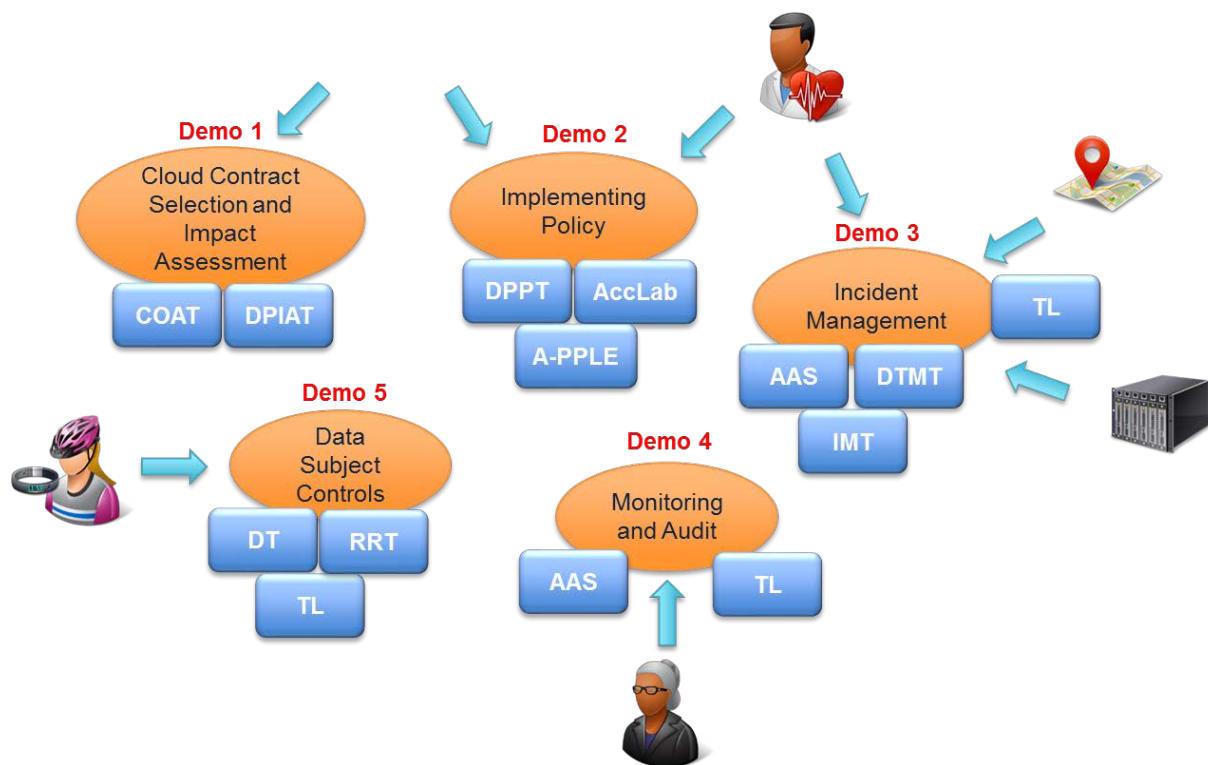


Figure 20: The demonstration scenarios of the wearables use case

Thus, we can define the following demonstration scenarios:

- **Demo Scenario 1: Selection of the cloud service supply chain**

This scenario presents the perspective of the Wearable Co as a cloud customer to demonstrate accountability in the policy definition and validation support service, as shown in Figure 21. In detail, the scenario refers to the selection of a compliant cloud service provider (Kardio-Mon in our case), based on their advertised capabilities for addressing specific functional, security and privacy requirements. In this scenario, we, also, present the angle of the Wearable Co to perform a data protection impact assessment on their decision to run their wearable business on the cloud, which includes processing of the personal data of the Wearable Co customers collected from their wearable devices. The impact assessment is based on a risk assessment approach, in which we demonstrate how the obligations and the requirements of the Wearable Co lead the assessment of the Kardio-Mon operations (and their third parties' operations on Map-on-Web and DataSpacer) to run the wearable service on behalf of the Wearable Co.

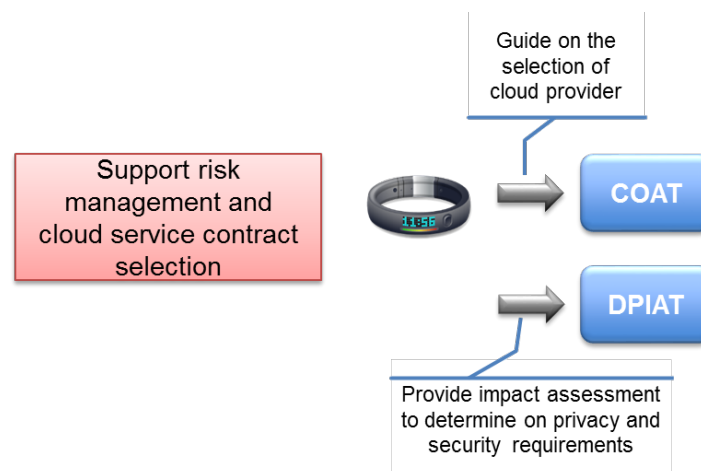


Figure 21: Summary of Demo Scenario 1 for the selection of the cloud service supply chain

▪ Demo Scenario 2: Implementation of policies

This scenario presents the perspective of Kardio-Mon to demonstrate accountability in the policy definition and validation support service and the policy management and enforcement service as well. In detail, the scenario refers to the development of the accountability machine readable policies, which govern the operation of the wearable service instance offered by Kardio-Mon for the Wearable Co. It, also, presents the implementation management and the enforcement of the policies in A-PPLE, so that they are used to configure the wearable service. Figure 22 summarises this demonstration scenario.

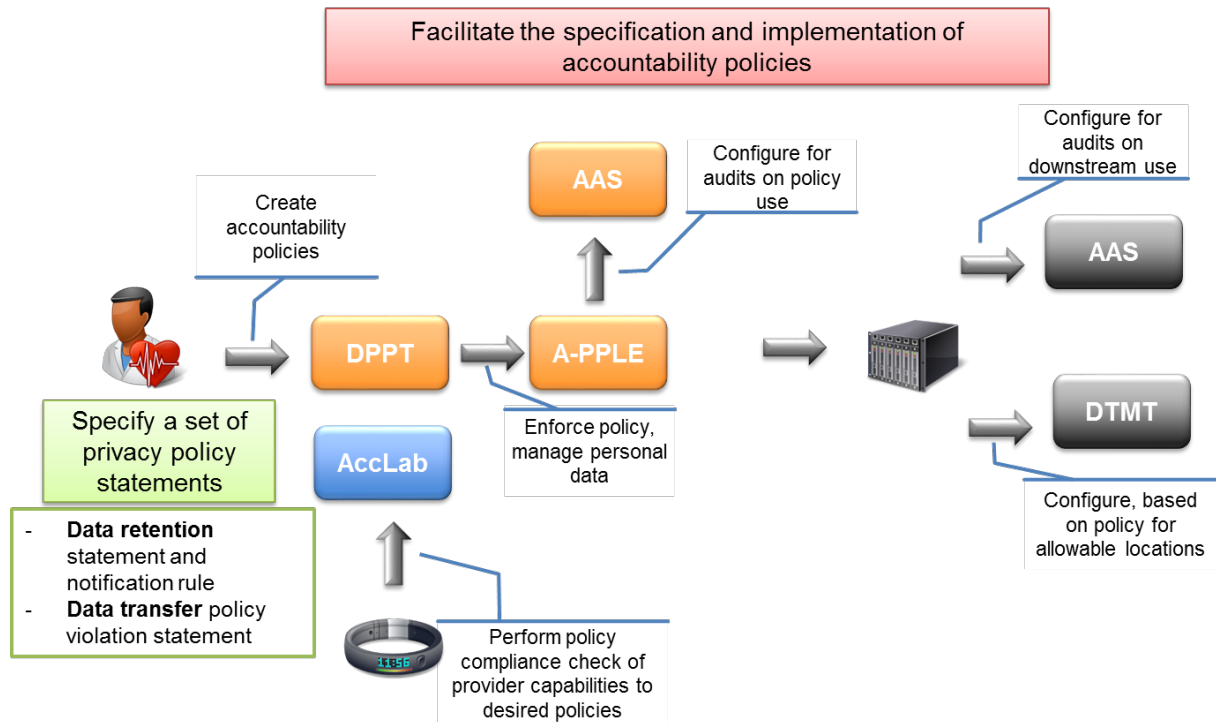


Figure 22: Summary of Demo Scenario 2 for the policy implementation

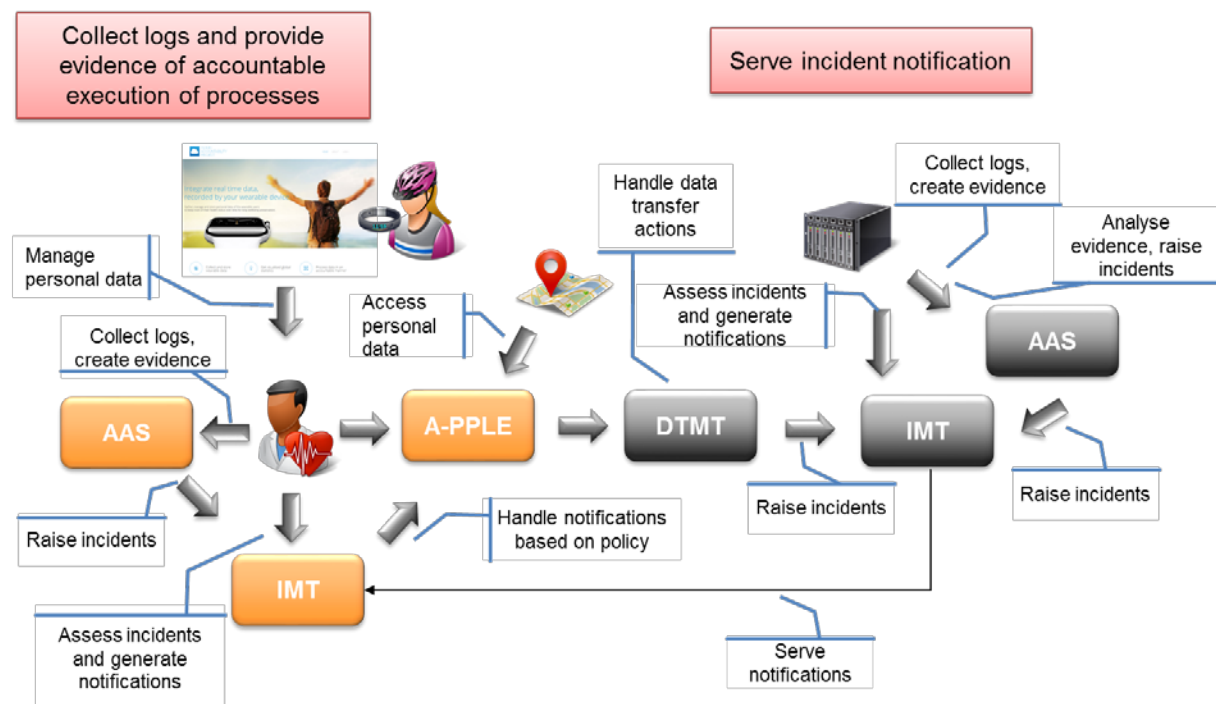


Figure 23: Summary of Demo Scenario 3 for incident management

▪ Demo Scenario 3: Incident Management

This scenario emphasizes on the perspective of the different actors in the cloud environment, namely Kardio-Mon, Map-on-Web and DataSpacer, to demonstrate their activities towards the collection of logs and the provision of evidence for the accountable execution of their processes. The activities in this scenario aim to demonstrate the involvement of these cloud providers in the monitoring and environment state collection, the collection and management of evidence, the incident management and the notification accountability support services. In that respect, this scenario places emphasis on how the cloud service supply chain behaves in cases that incidents (like data breaches or policy violations) happening in the cloud environment disturb the end-to-end operation of the wearable service. Figure 23 summarises this demonstration scenario.

▪ Demo Scenario 4: Monitoring and Audit

This scenario presents the perspective of the Cloud Auditor and the Cloud Supervisory Authority to perform audits on the data handling procedures of the cloud providers. Thus, the scenario refers to the validation accountability support services and presents the ability of Kardio-Mon and DataSpacer to provide evidence on the accountable execution of their processes, in cases that the Cloud Auditor is asked to audit these providers for incidents about: i) an intrusion detection incident on Kardio-Mon, ii) an incomplete application of a data retention policy enforcement scenario between Kardio-Mon and DataSpacer, and iii) an unallowable data transfer incident on DataSpacer.

Figure 24 summarises this demonstration scenario.

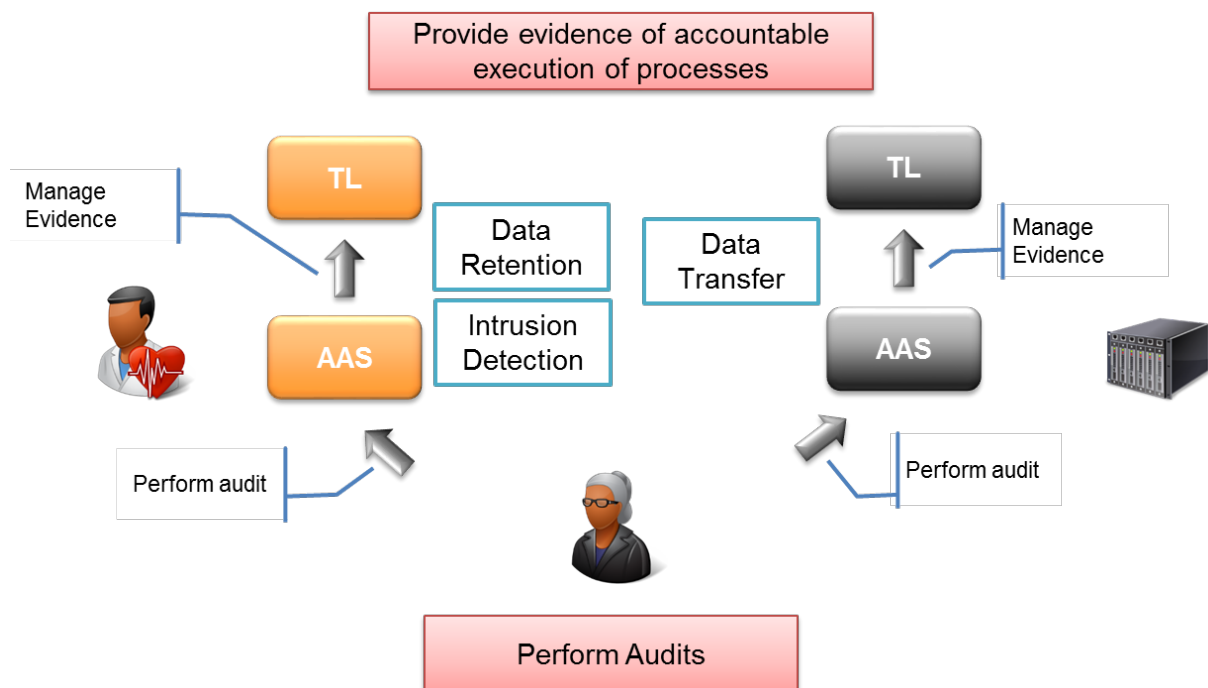


Figure 24: Summary of Demo Scenario 4 for monitoring and audit

▪ Demo Scenario 5: Data Subject Controls

This scenario presents the perspective of the Wearable Co customer as the cloud subject in the wearables use case. The scenario facilitates the requirements of the validation accountability support service, in which the Wearable Co customer is able to handle the disclosure of the personal data collected from the Wearable application and the wearable device to the cloud and, specifically, to Kardio-Mon. This scenario, also, addresses the remediation accountability support service, in which the Wearable Co customer is notified of incidents occurred in the cloud environment of Kardio-Mon and their third parties, Map-on-Web and DataSpacer, and is prompted for adopting the most relevant remedies.

Figure 25 summarises this demonstration scenario.

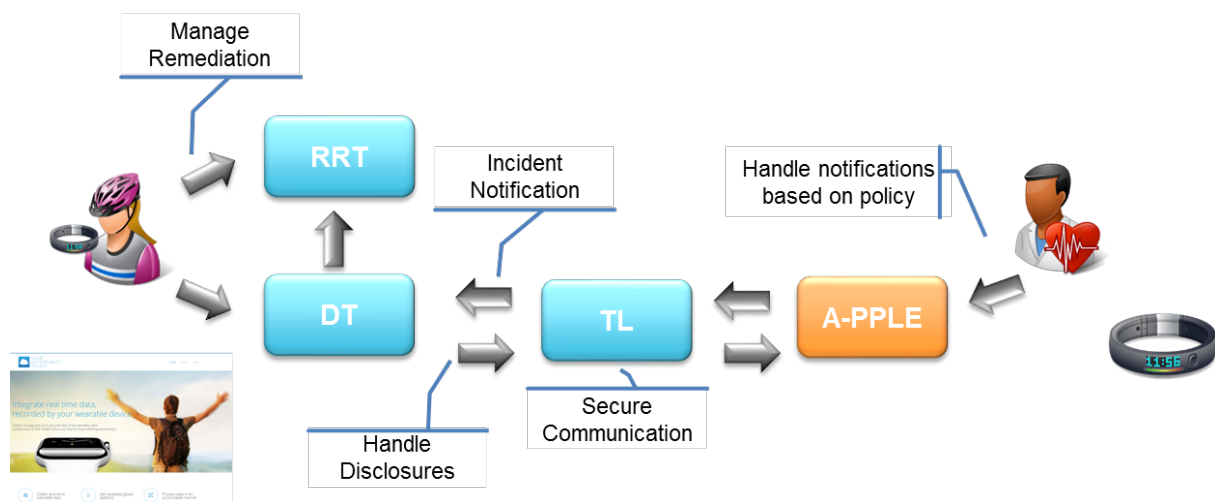


Figure 25: Summary of Demo Scenario 5 for data subject controls

In the following sections we elaborate on these scenarios, based on the following template:

- The scope of the demonstration scenario: it provides a short overview on why we introduce this scenario in order to demonstrate the final A4Cloud use case prototype. It, also, highlights the need of the assigned primary cloud role for implementing specific accountability support services in the scenario and how the A4Cloud tools support this implementation.
- The involved business actors from the wearables use case, emphasising on who is the primary cloud actor(s).
- A high level story on how this scenario is evolved.
- A summary of how the demonstration scenario addresses the accountability framework by referring to the accountability processes, support services and artefacts reflected in the scenario.
- Any dependencies of the scenario to other demonstration scenarios or any external prerequisites, like existing documents or accountability artefacts.
- The steps realised for the accomplishment of the demonstration scenario. In these steps, we highlight the use of the A4Cloud by the respective actor, what the tools require as input in every step of the scenario and which is output received.
- A summary on what we achieved by presenting this demonstration scenario as part of the A4Cloud final use case prototype.

5.2 Demo Scenario 1: Selection of the cloud service supply chain

This scenario presents the perspective of the Wearable Co.

5.2.1 Scope

When a cloud customer search for services offered by cloud providers, traditional brokerage tools focus on finding matches based merely on functional requirements. COAT enables the cloud customer to make an informed choice of an appropriate cloud service provider on the basis of a set of data protection and privacy requirements. Through a filtering process of the relevant clauses, the tool simplifies reviewing of complex cloud contracts. The tool informs the user beforehand on the consequences following from setting a specific requirement (e.g. allowing storage of personal data outside the EEA). Ultimately, cloud customers understand in a clear manner what they are signing for.

Furthermore, as part of the new General Data protection regulation (GDPR), several cloud customers will have to perform a data protection impact assessment (DPIA) before they use a cloud service provider. This process of assessment allows cloud customers (largely considered as data controllers) to evaluate the risks when assigning a cloud service provider (mostly considered as data processor)

with a particular set of processing operations (project). To this end, DPIAT assists cloud customers in many ways: it helps them identify both compliance issues with the data protection rules and possible threats for individuals, while raising the overall awareness of tool users with respect to data protection matters.

5.2.2 Actors Involved

COAT is -primarily- addressed to Small and Medium Enterprises (SMEs), acting in their capacity as cloud customers. The tool is designed to be used by individual users, though, not necessarily by IT or legal experts. Actors involved are business experts who act as cloud customers. In the context of the wearables use case scenario, COAT is used by the **Wearable Co** (cloud customer) providing assistance in searching for an appropriate cloud service provider. On the basis of the requirements set by the **Wearable Co**, the tool indicates **Kardio-Mon** as the appropriate provider to serve the requirements of the **Wearable Co**.

The DPIAT -primarily- targets SMEs acting in their capacity as (potential cloud customers²). With respect to the wearables use case, the primary cloud actor(s) involved in this scenario using DPIAT is the **Wearable Co** (cloud customer) aiming to get assistance in assessing the risks of using, in this case, a pre-selected, cloud service provider, namely **Kardio-Mon** and **Data Spacer**.

5.2.3 Description of the demo scenario

The Wearable Co as a cloud customer is looking for a cloud SaaS provider who will take care of the provision of a cloud service for the Wearable Co, considering cloud storage and data protection requirements. A Wearable Co employee uses COAT to search for a matching service provider. Upon this selection, the Wearable Co assesses the risks of selecting Kardio-Mon, as their cloud service provider.

5.2.4 Addressing the Accountability Framework

Both COAT and DPIAT support the “risk management and cloud service contract selection” accountability process. They are part of the preventive accountability mechanisms and implement the policy definition and validation accountability support service.

The main input of this scenario is the capabilities artefacts, which are exploited by COAT and DPIAT to operate their expected functionality, offered in this scenario.

This scenario is based on the interactions shown in Figure 3.

5.2.5 Prerequisites

Prior to demonstration of this scenario and the use of COAT and DPIAT by the Wearable Co employee, the operator of the tools should have populated a knowledge base with the different kinds of offers from the various cloud service providers.

5.2.6 The scenario steps

The execution of this demonstration scenario is split into the phases, in which the Wearable Co employee first selects a cloud provider and, subsequently, perform a DPIA to assess this selection.

We start with the use of COAT. Figure 26 presents the information flow between the Wearable Co (as customer) and the tool in order to assess the capabilities of the cloud service providers. As shown there, the Wearable Co employee uses as follows:

- (1) The Wearable Co (the cloud customer) launches the COAT-tool (see Figure 27).

² Note that DPIAT was originally designed presuming that the cloud customer has not yet selected a cloud service provider. DPIAT, however, can be used as well following the selection of a cloud service provider through COAT.

- (2) The Wearable Co picks the service type they are searching for. In this case Content Management, Social Network, and Collaboration (see Figure 28).
- (3) Based on the selected service type, the Wearable Co is presented a list of the suggested cloud providers (see Figure 29).
- (4) Now the cloud customer, Wearable Co, has the opportunity to make a narrower filtering among these cloud providers by specifying certain geographical locations for data storage, backup, processing of personal data, encryption, court of choice, deletion, etc. Among the requirements, the cloud customer can specify, for instance, whether it allows the primary cloud service provider to subcontract with third parties regarding the offerings of services such as storage of data by providers of IaaS.
- (5) When the Wearable Co has done all the specific customisations, the tool presents a list of cloud service providers, including Kardio-Mon, meeting the data protection and privacy requirements set throughout the matching process (see Figure 30).
- (6) Finally, it rests with the user of COAT to decide at the end whether Kardio-Mon is, indeed, the most appropriate cloud service provider for the type of service requested by Wearable Co.

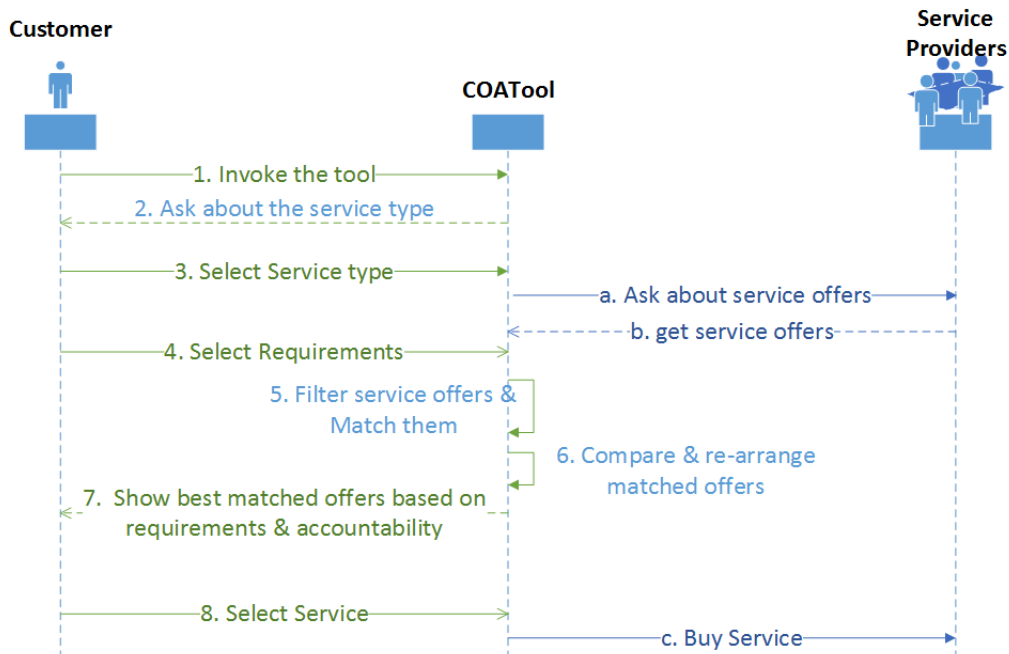


Figure 26: The information flow for using the COAT in demo scenario 1.

Cloud Offerings Advisor

Please indicate your requirements

Where are you?:

United Kingdom ▼

We have tried to guess your location. Please change this if we got it wrong.

Who are you?:

Business

Consumer

Figure 27: Demo scenario 1 – accessing the COAT tool.

Please indicate your requirements

What types of services do you need?

Software
as a service

- ☐ Billing
- ☐ CRM (Customer Relation Management)
- ☐ Collaboration
- ☐ Content Management
- ☐ Digital Media
- ☐ Document Management
- ☐ ERP (Enterprise Resource Planning)
- ☐ Emails and Office Productivity
- ☐ Financials
- ☐ Human Resources and Sales
- ☐ Manufacturing
- ☐ Order Management
- ☐ Portals/Search
- ☐ Social Network
- ☐ Utilities/Management

Platform
as a service

- ☐ Application Deployment
- ☐ Business Analysis
- ☐ Business Intelligence
- ☐ Databases
- ☐ Development & Testing
- ☐ Networks Operations
- ☐ Open and Custom Clouds Platforms
- ☐ Web Hosting

Infrastructure
as a service

- ☐ Backup & Recovery
- ☐ Communication
- ☐ Computing
- ☐ Infrastructure Service Management
- ☒ Storage
- ☐ Virtualisation

Other Services

- ☒ Integration
- ☐ Metadata
- ☐ Security
- ☐ Service-bus

Back Continue

Figure 28: Demo scenario 1 – selecting the types of services in the COAT tool.

Advisor

Business Questionnaire

Please indicate your requirements

Price Range

From: € 0 To: € 5000

Acceptable Storage Locations including Backup

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

Acceptable Data processor location

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

Data transfer in case of emergency? ☐

Do you want Encryption?

- ☐ Yes
- ☐ No
- ☐ Doesn't Matter

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

- ☐ Yes
- ☐ No

Should unlimited backup be included? ☐

Notified in case of security breach? ☐

8 Matched Offers

Cirrus Thinking

€10.00/Month

Storage Location: Processor Location: client-side encryption

More info Go to offer

Cloud Corner

€50.00/Month

Storage Location: Processor Location: client-side encryption

More info Go to offer

Acceptable Data processor location

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

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

€7.50/Month

Storage Location: Processor Location: client-side encryption

More info Go to offer

€7.37/Month

Storage Location: Processor Location: 256bit aes

More info Go to offer

Dropbox

€50.00/Month

Storage Location: Processor Location: 256bit aes

More info Go to offer

Jottacloud

€6.00/Month

Storage Location: Processor Location: client-side encryption

More info Go to offer

Figure 29: Demo scenario 1 – indicating requirements in the COAT tool.

Cloud Offerings Advisor

country?

☐ No

☐ Yes

Should unlimited backup be included? ☐

Notified in case of security breach? ☐

Deletion: Control over deletion of your data?

☐ I Trigger Deletion

☐ Provider can delete in case of termination

☐ Insurance of hard deletion (overwriting the hard-drive)

Transparency: in case of changing terms and conditions

☐ Notified well in advance

☐ Have the right to terminate

☐ Vendor can't change terms of agreement

Service Provider has certificate? ☐

Engagement Period: length of contract

☐ Open

☐ 6 Months

☐ 1 Year

☐ 3 Years

Notified when Law Enforcement requests your data (if legally possible)? ☐

IPR on user content

☐ Remains with Client

☐ May be used by the Cloud Provider

Dropbox Storage Location Processor Location 256bit x256 [More info](#) [Go to offer](#)

Jottacloud €6.00/Month Storage Location Processor Location x256 [More info](#) [Go to offer](#)

Kar €10.00/Month Storage Location Processor Location 256bit x256 [More info](#) [Go to offer](#)

Kardio-Mon €10.00/Month Storage Location Processor Location strong 2014 [More info](#) [Go to offer](#)

Teamdrive €5.02/Month Storage Location Processor Location strong 2014 or better [More info](#) [Go to offer](#)

Figure 30: Demo scenario 1 – selecting Kardio-Mon in the COAT tool

At the end of the selection process, the cloud customer, in this case the Wearable Co, has been able to find a good match, in this case Kardio-Mon, based on their data protection and privacy requirements. In order to find this match, the Wearable Co have looked into information, regarding the specific cloud offering, have accessed the actual contract and, eventually, have made an informed choice of Kardio-Mon. Thus, COAT has enabled the Wearable Co to save resources; a well-informed decision for an appropriate cloud service provider was taken in an efficient manner without seeking external expertise.

The next step is to assess the risks for personal data relating to the use of Kardio-Mon, as selected provider for services linking to a particular project to be conducted within the Wearable Co; DPIAT contributes to such assessment. Thus, the Wearable Co employee uses DPIAT as following:

- (1) The Wearable Co employee launches the DPIA tool and selects their chosen service provider, in this case Kardio-Mon, from the drop-down menu (see Figure 31).
- (2) The Wearable Co starts off by doing the Pre-Screening Questions, which is a questionnaire consisting of six (6) questions to determine whether a full screening is needed. Depending on the outcome of the Pre-Screening questions, DPIAT will recommend the Wearable Co or not to proceed with the full screening, consisting of a larger set of fifty (50).
- (3) The Wearable Co is advised to do the full Screening Questions and is directed to a set of questions covering different areas such as, for instance, the type of project to be assigned to the cloud service provider (see Figure 32), the type of data processed (see Figure 33), the transfers of information, as well as questions that are specific to the cloud environment (see Figure 34).
- (4) After the Screening Questions, the Wearable Co is now presented to the risk evaluation, divided into 3 categories (see Figure 35): Risks related to the project or application which the customer will develop (see Figure 36), risks related to the selected CSP (see Figure 37), in this case Kardio-Mon, and information regarding the data protection process especially in relation to the new General Data Protection Regulation.
- (5) Given these results, the Wearable co decides to choose Kardio-Mon as their Cloud Service Provider.

A4 Cloud Data Protection Impact Assessment Tool

Please choose a Questionnaire

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

Select a service provider

Map-On-Web

Pre-Screening Questions

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

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

[take this questionnaire](#)

Screening Questions

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

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

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

[take this questionnaire](#)

Disclaimer

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

Nothing in this tool is intended to be an invitation or inducement to engage or enter into, or advice against engaging or entering into, an undertaking of any kind.

The content or information displayed in this tool is for general informational purposes regarding compliance with the applicable data protection laws only.

A4Cloud shall not be liable for any damages resulting from the use of the tool, including damages caused by any incorrectness or incompleteness of information provided on the tool. The content provided in the tool does not necessarily represent the

Figure 31: Demo scenario 1 – accessing DPIAT and selecting preferred cloud service provider for analysis.

The aim of this set of questions is to assess in a granular manner how the interactions between you and the CSP you deal with impact your users' rights to privacy.

You are to answer all questions to the best of your knowledge, if necessary asking the relevant professionals in your undertaking before answering; some questions

Type of Project

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

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

☐ Yes
☐ No

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

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

- ☐ Account and/or Subscription Management
- ☐ Advertising, Marketing and/or Promotion
- ☐ Authentication and Authorization
- ☐ Banking and Financial Management
- ☐ Charitable Donations
- ☐ Communications Services
- ☐ Customization
- ☐ (Service) Delivery
- ☐ Education Services
- ☐ Government Services
- ☐ Healthcare Services
- ☐ News and Information - Arts and Entertainment
- ☐ Online Gambling
- ☐ Online Gaming
- ☐ Payment and Transaction Facilitation
- ☐ Recruitment and Hiring

Figure 32: Demo scenario 1 – screenshot from DPIAT to the type of project.

Collection and Use of Information

4: Are you relying exclusively on consent in order to process information of individuals?

Consent means 'any freely given specific, informed and explicit indication of his or her wishes by which the individual either by a statement or by a clear affirmative action signifies agreement to information relating to them being processed.'

- ☐ Yes
- ☐ No

5: How have you obtained the consent of individuals?

Consent requires prior information and an explicit indication of the intent to consent.

- ☐ Consent is given directly by the individual by a statement (e.g. by a consent form)
- ☐ Consent is given directly by the individual by an affirmative action (e.g. by ticking a box)
- ☐ Consent has been obtained implicitly by the individual (e.g. by merely use of the service or inactivity)

6: If individuals have given their consent, can they withdraw it with ease and whenever they want to?

Consent means 'any freely given specific, informed and explicit indication of his or her wishes by which the individual either by a statement or by a clear affirmative action signifies agreement to information relating to them being processed.'

- ☐ Yes
- ☐ No

7: Are the consequences of withdrawal of consent significant for individuals?

For instance, will the service to the individual be terminated, while the individual depends on it?

- ☐ Yes
- ☐ No

8: On what basis do you process the information?

Figure 33: Demo scenario 1 – screenshot from DPIAT on the collection and use of information.

Cloud Specific Questions

48: The cloud infrastructure (hardware and/or software) I use is:

The potential threats to privacy and protection of personal information are influenced by the deployment model of the CSP. This means that the risk is higher if the number of the subjects who operate in the system is also high.

- ☐ Owned by or operated for only me (private cloud)
- ☐ Is owned by or operated for a specific group of users with common interests in a shared manner (community cloud)
- ☐ Is shared amongst multiple users (public cloud)

49: Does the service that you use consist of the provision of end user applications run by the cloud service provider?

Think for instance of Salesforce CRM or Wuola.

- ☐ Yes
- ☐ No
- ☐ I don't know

50: Are specific arrangements in place with regards to your information in case you want to terminate or transfer the cloud service?

The application of such rules/procedures gives you the ability to have control/access over the information you process. For instance, you can transfer the information you process to another provider if needs be (bankruptcy, force majeure etc).

- ☐ Yes
- ☐ No
- ☐ I don't know

[Previous](#) [Finish](#)

Figure 34: Demo scenario 1 – screenshot from DPIAT on cloud specific questions.

A4 Cloud Data Protection Impact Assessment Tool

Questionnaire Results (selected Cloud Service Provider: [Kardio-mon](#))

MEDIUM
Risk Related to Your Proposed Application

Risk Related to the selected Cloud Service Provider

Usage of this Report within a Broader Data Protection Impact Assessment (DPIA) Process

Disclaimer

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

Nothing in this tool is intended to be an invitation or inducement to engage or enter into, or advice against engaging or entering into, an undertaking of any kind.

The content or information displayed in this tool is for general informational purposes regarding compliance with the applicable data protection laws only.

A4Cloud shall not be liable for any damages resulting from the use of the tool, including damages caused by any incorrectness or incompleteness of information provided on the tool. The content provided in the tool does not necessarily represent the state-of-the-art and A4Cloud may update it as necessary without prior notice.

If you want more information about compliance with data protection laws in respect of the information you input into the tool, you will need to contact the relevant authorities.

Figure 35: Demo scenario 1 – screenshot from DPIAT on risk evaluation.

A4 Cloud Data Protection Impact Assessment Tool

Questionnaire Results (selected Cloud Service Provider: [Kardio-mon](#))

MEDIUM
Risk Related to Your Proposed Application

Sensitivity	MEDIUM	Risks related to a sensitive market (i.e. elderly, children, etc.) and/or sensitive data (i.e. health or medical conditions, finance, sexual behaviour)
Compliance	HIGH	Risks related to compliance with external standards, policies, laws, etc.
Trans-Border Data Flow	LOW	Risks related to transfer of information across national borders
Transparency	HIGH	Risks related to transparency in the areas of notice/user messaging and choice/consent
Data Control	MEDIUM	Risks related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention)
Security	MEDIUM	Risks related to security of data and data flows
Data Sharing	LOW	Risks related to sharing data with third parties

Risk Related to the selected Cloud Service Provider

Usage of this Report within a Broader Data Protection Impact Assessment (DPIA) Process

Figure 36: Demo scenario 1 – screenshot from DPIAT on the results for the risks related to the wearable service.

A4 Cloud Data Protection Impact Assessment Tool

Questionnaire Results (selected Cloud Service Provider: Kardio-mon)

<div> <div> <div></div> <div>MEDIUM</div> </div> <div>Risk Related to Your Proposed Application</div> </div>			
<div> <div> <div></div> <div></div> </div> <div>Risk Related to the selected Cloud Service Provider</div> </div>			
Policy & Organizational			EXTREMELY LOW
R-01	R.1 lock-in		VERY LOW
R-02	R.2 loss of governance		LOW
R-03	R.3 compliance challenges		VERY LOW
R-04	R.4 loss of business reputation due to co-tenant activities		VERY LOW
R-05	R.5 cloud service termination or failure		LOW
R-06	R.6 cloud provider acquisition		EXTREMELY LOW
R-07	R.7 supply chain failure		EXTREMELY LOW
Technical			VERY LOW
R-08	R.8 resource exhaustion (under or over provisioning)		VERY LOW
R-09	R.9 isolation failure		VERY LOW
R-10	R.10 cloud provider malicious insider - abuse of high privilege roles		VERY LOW
R-11	R.11 management interface compromise		VERY LOW
R-12	R.12 intercepting data in transit		VERY LOW
R-13	R.13 data leakage on up/download intra-cloud		VERY LOW
R-14	R.14 insecure or ineffective deletion of data		VERY LOW
R-15	R.15 distributed denial of service (ddos)		VERY LOW
R-16	R.16 economic denial of service (eddos)		VERY LOW
R-17	R.17 loss of encryption keys		VERY LOW
R-18	R.18 undertaking malicious probes or scans		VERY LOW
R-19	R.19 compromise service engine		VERY LOW
R-20	R.20 conflicts between customer hardening procedures and cloud environment		EXTREMELY LOW
Legal			VERY LOW

Figure 37: Demo scenario 1 – screenshot from DPIAT on the results for the risks related to Kardio-Mon.

5.2.7 Outcome

Through this scenario, the Wearable Co is able to choose Kardio-Mon, as the cloud service provider to operate the proposed wearable service application. This outcome is achieved after the Wearable Co has been guided through selecting the capabilities of Kardio-Mon to meet the claimed functional, data protection and privacy requirements and performing a DPIA to evaluate the risks involved in using Kardio-Mon as a cloud service provider for this project. The report has three categories: the first is risks related to the application that the Wearable Co wants to operationally support, the second part is the risks related to the use of Kardio-Mon as the particular cloud service provider, and the final part is information regarding the overall data protection impact assessment process, part of which is the report produced by the DPIAT tool.

5.3 Demo Scenario 2: Implementation of policies

This scenario presents the perspective of Kardio-Mon to develop accountability policies, after collaborating with the Wearable Co.

5.3.1 Scope

This scenario focuses on a CSP that has to set up the policy enforcement components. The aim of this demo scenario is to show how DPPT automates the task for the implementation of the accountability-related policies. The CSP has to specify the policies through the GUI and, then, DPPT handles the translation of the selected policies in the language used by the enforcement components. The CSP can also use DPPT when they need to enact the policies. In fact, DPPT is integrated with A-PPLE and can interact with it when the CSP decide to enforce the policies.

The scenario involves the specification of the formal privacy statements and their logical meaning via the use of AccLab. This tool is used by the privacy officers to write privacy and accountability requirements of the wearables use case, in a more rigorous style. These formal statements are then

checked for consistency and finally the privacy officer can establish the compliance between an offer from a cloud provider, like Kardio-Mon, and a policy required from a customer, like the Wearable Co.

5.3.2 Actors Involved

With reference to the wearable use case, Kardio-Mon (potentially a privacy officer) is the primary actor to be involved in this scenario. Kardio-Mon is the data processor that has been selected by Wearable Co, and plays the role of the data controller. The Kardio-Mon cloud service offers statistics about health related parameters and needs to process personal data belonging to users that register to the platform. Kardio-Mon own the instance of the policy enforcement engine (A-PPLE), therefore they need to enforce policies that should be applied to the processing of the personal data.

Apart from Kardio-Mon, the privacy expert employed by the Wearable Co is another, involved in the scenario, with the task to check the final policy against the capabilities of Kardio-Mon and the initial requirements raised by the Wearable Co.

5.3.3 Description of the demo scenario

Kardio-Mon, being a CSP processing personal data, need to set up the environment for the enforcement of the policies that apply to the processing of personal data. Kardio-Mon use DPPT to select and specify the policies that apply to the service being provided. Through the GUI offered by DPPT, the Kardio-Mon privacy officer specifies different data protection related aspects, such as data collection, data retention, data access control and data breach notification, etc.

When all aspects are specified, the Kardio-Mon privacy officer uses DPPT to generate the policy file, which is a representation of the accountability related policies in A-PPL language. This machine readable form of the policy is sent to the privacy expert of the Wearable Co, who, in turn, needs to get guarantees about its policies. For instance, the privacy expert wants to get insurance about its privacy requirements. Thus, after formalizing the information coming from DPPT, they can check that these requirements are consistent. In a second step, the privacy expert of the Wearable Co may want to verify that the policy offer, as defined by Kardio-Mon, is formally compliant with the requirements set by the Wearable Co.

The above communication may be repeated, so that Kardio-Mon and the Wearable Co result in an agreed set of policies. When these policies need to be enforced, Kardio-Mon can use DPPT to send the policy to the A-PPLE engine in charge of the enforcement.

5.3.4 Addressing the Accountability Framework

The tools involved in this demonstration scenarios, DPPT and AccLab, help Kardio-Mon and the Wearable Co cover the *Define Policies* and part of the *Enforce Policies* phases of the accountability lifecycle and implement the associated accountability support services, namely the policy definition and validation and the policy management and enforcement. The definition of the policies is done by specifying them through the DPPT GUI. The part of the enforcement phase, which is covered by using DPPT, is about the set up and configuration of the enforcement tools. Furthermore, AccLab helps in writing formal privacy and accountability requirements and then checking them for consistency and compliance. One classic problem in writing policies is the presence of conflicts, towards which AccLab aims to provide assistance in localizing these potential conflicts in the policy specification.

This scenario is based on the interactions shown in Figure 4 and Figure 5.

5.3.5 Prerequisites

Before executing this scenario and using DPPT, Kardio-Mon needs to have the results of the analysis of the risks involved in carrying out the processing personal data, and the privacy related requirements that are part of the agreement with the Wearable Co. Therefore, it is assumed that what Kardio-Mon specifies through DPPT reflects the contractual and legal requirements in place.

5.3.6 The scenario steps

Kardio-Mon uses DPPT as a standalone tool. The first step is the identification of the service, to which the policies being specified apply. The identifier is made of the two fields called Service Name and Cloud Service Provider, as shown at the top of Figure 38.

Figure 38: Demo scenario 2 - Specification of Service Name and Cloud Service Provider fields in DPPT.

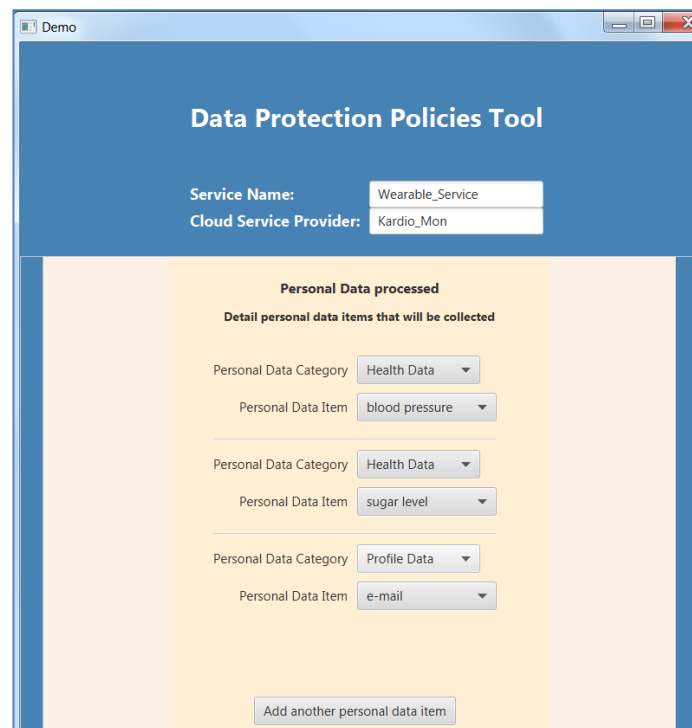
Kardio-Mon uses the sections in the graphical interface to specify different data protection aspects related to the processing of the personal data. Specifically, Kardio-Mon defines the following information:

- The personal data items that will be collected and processed, along with the purpose. Examples of these data are blood pressure, heart rate, sugar level, username, email address. The purpose in this case is to provide Health Stats.
- The data retention period, after which personal data need to be deleted.
- The access control rights granted to the actors involved in the processing activities (for example, other actors in the chain, such as sub-processors)
- Notifications that need to be sent when specific processing related events occur. Examples of such events are data transfer violation and access denied.
- Data transfer aspect, which includes the country where data may be transferred and the legal ground for the transfer.

Figure 39 shows the interface used by Kardio-Mon to provide details about the personal data that will be collected. Figure 40 shows the Data Transfer section of the DPPT.

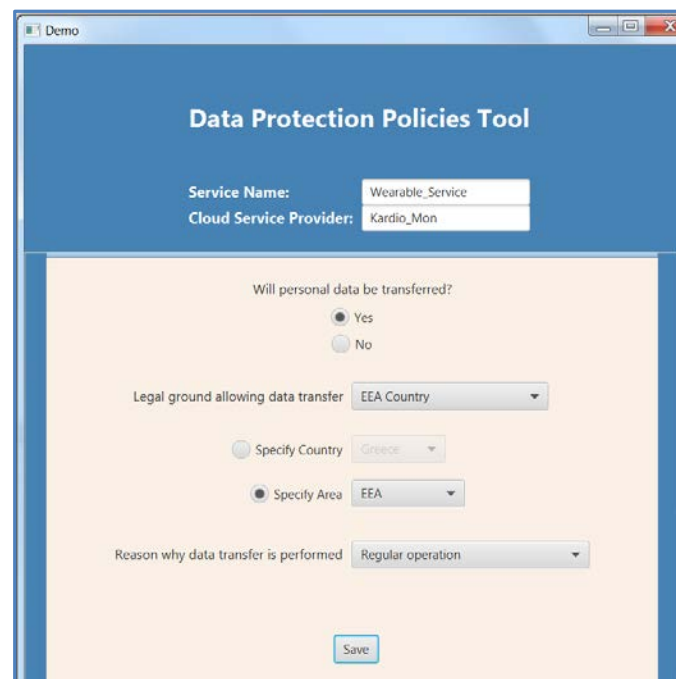
When Kardio-Mon has completed the specification of the policies, it can produce the A-PPL policy file, which represents the policies specified by Kardio-Mon in the A-PPL language. This is done by using the *Create A-PPL Policy* button (highlighted with a yellow rounded rectangle at the bottom of Figure 41).

DPPT can also produce a different representation of the policy (ontology-based) that can be used to expose in a machine understandable form the policies offered by Kardio-Mon for the Wearable Service. This representation is used by AccLab to check whether the available services offer policy compliant with cloud customers' requirements.



The screenshot shows a web application window titled "Demo" with the header "Data Protection Policies Tool". Below the header, there are two input fields: "Service Name:" with the value "Wearable_Service" and "Cloud Service Provider:" with the value "Kardio_Mon". The main content area is titled "Personal Data processed" and contains the sub-header "Detail personal data items that will be collected". There are three rows of data entry, each with a "Personal Data Category" dropdown and a "Personal Data Item" dropdown. The first row has "Health Data" for the category and "blood pressure" for the item. The second row has "Health Data" for the category and "sugar level" for the item. The third row has "Profile Data" for the category and "e-mail" for the item. At the bottom of the form, there is a button labeled "Add another personal data item".

Figure 39: Demo scenario 2 - Specification of personal data elements collected



The screenshot shows the same web application window as Figure 39, but with a different form. The header and input fields for "Service Name" and "Cloud Service Provider" are the same. The main content area is titled "Data Protection Policies Tool" and contains the sub-header "Will personal data be transferred?". There are two radio buttons: "Yes" (selected) and "No". Below this, there is a "Legal ground allowing data transfer" dropdown menu with the value "EEA Country". There are two more radio buttons: "Specify Country" and "Specify Area" (selected). The "Specify Country" option has a dropdown menu with the value "Greece". The "Specify Area" option has a dropdown menu with the value "EEA". Below this, there is a "Reason why data transfer is performed" dropdown menu with the value "Regular operation". At the bottom of the form, there is a button labeled "Save".

Figure 40: Demo scenario 2 - Specification of Data Transfer policy



Figure 41: Demo scenario 2 - Buttons for the creation of the policy and for sending it to the A-PPL Engine

The privacy expert of the Wearable Co receives the policies. In order to check them against their requirements, the privacy expert needs to write the formal privacy requirements. For that, the expert uses the AccLab editor with syntax highlighting, auto-completion and templates features. The task is to translate the privacy related information coming from the policies defined through DPPT (see Figure 42). For instance, the data transfer clause states that transfers are permitted in EEA countries for any sensible data.

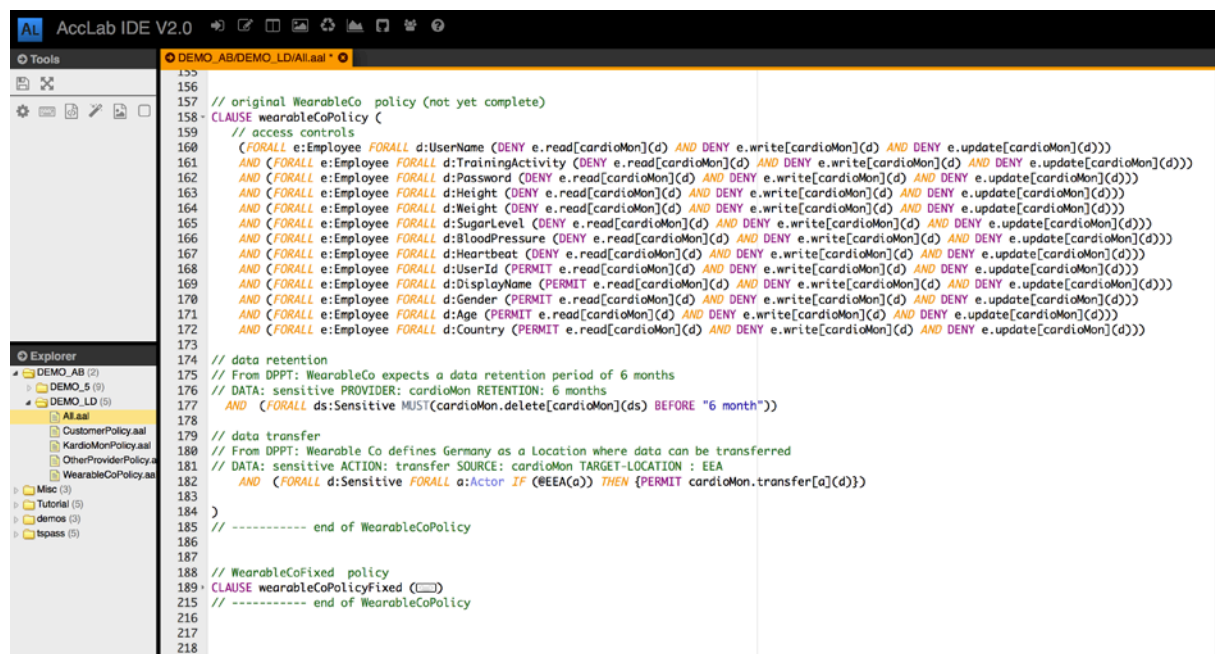


Figure 42: Demo scenario 2 – Specification of formal privacy requirements in AccLab.

Then, the privacy expert of the Wearable Co checks that the policy can be implemented. To this end, he uses the blue panel and the "satisfiability" option. In other words this AccLab option verifies if the clause is logically consistent or without conflict. Here the Wearable Co policy is satisfiable.

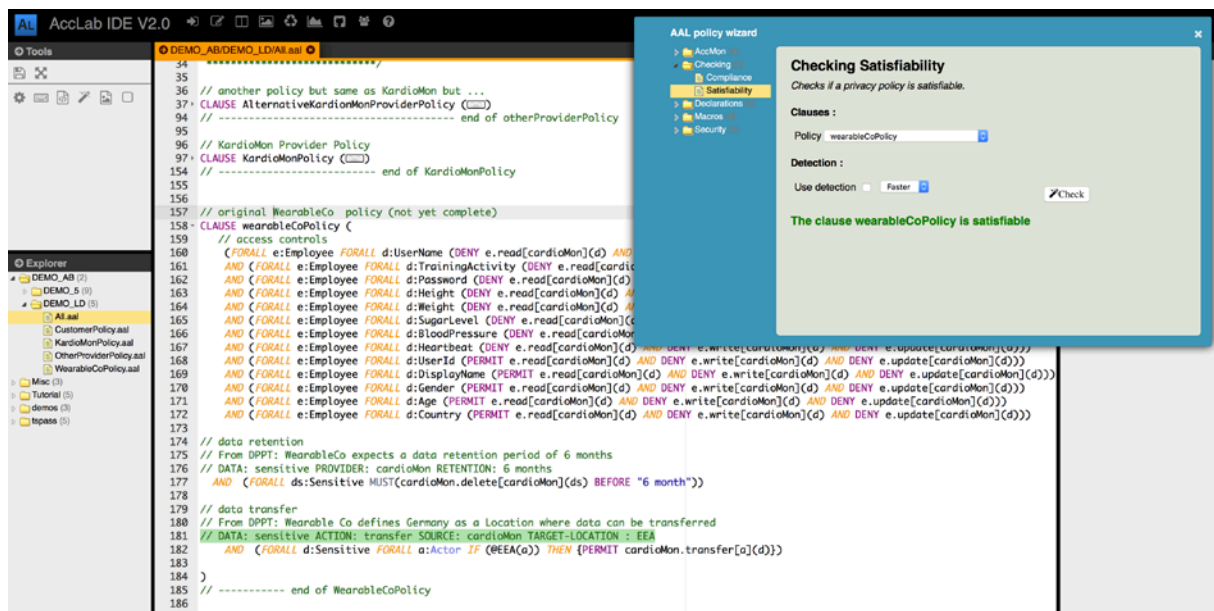


Figure 43: Demo scenario 2 – Satisfiability of the policy in AccLab.

Now the privacy expert of the Wearable Co wants to check the compliance of the Wearable Co requirements with the offer proposed by Kardio-Mon (see Figure 44). Several policies have been previously imported in the file and the compliance still uses the blue panel but with the "compliance" item. Unfortunately it fails.

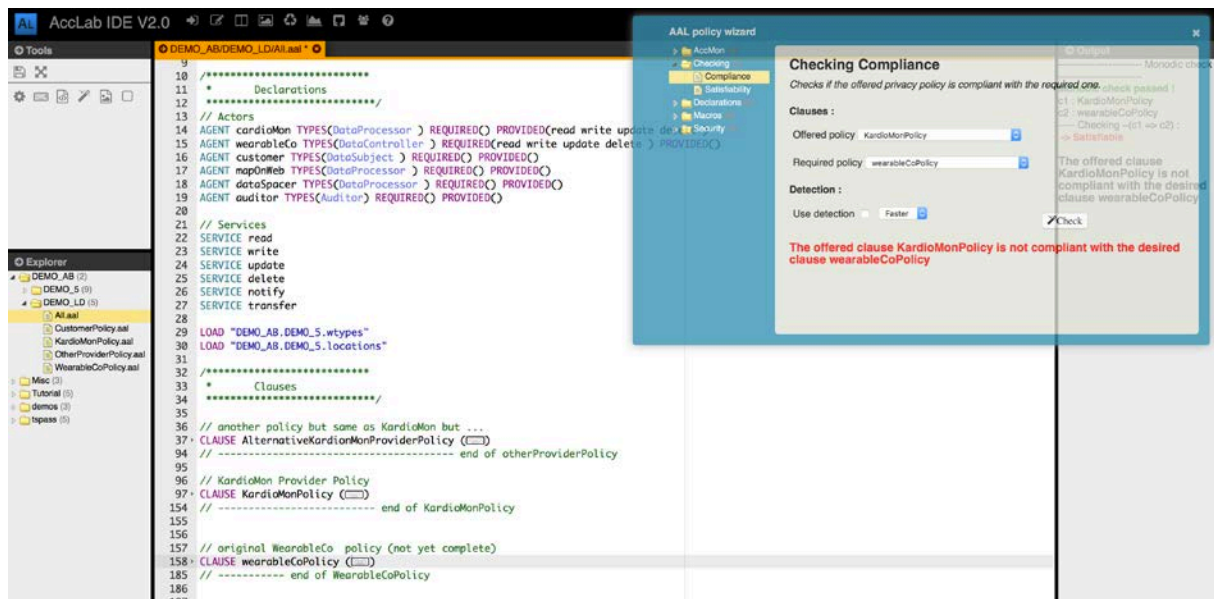


Figure 44: Demo scenario 2 – Policy compliance check in AccLab.

The AccLab tool provides some assistance in localizing conflicts by checking the "use detection" box. After one minute we get a precise result about what is the part of the clause which is not compliant. This is the data transfer location in line 182 (see Figure 45).

Thus, the privacy expert understands that the problem is the location, which is not compliant with the requirements in Kardio-Mon. Looking at the Kardio-Mon requirements, he can realise that "Russia" is not in EEA thus compliance cannot be achieved here (see Figure 46).

Therefore, the Wearable Co privacy expert has two choices to fix this situation: a) by changing the Wearable Co requirements or b) by changing the offered policy. He can fix the Wearable Co policy, with Russia or Croatia as target locations for instance, and, then, he checks that the compliance is correct (see Figure 47).

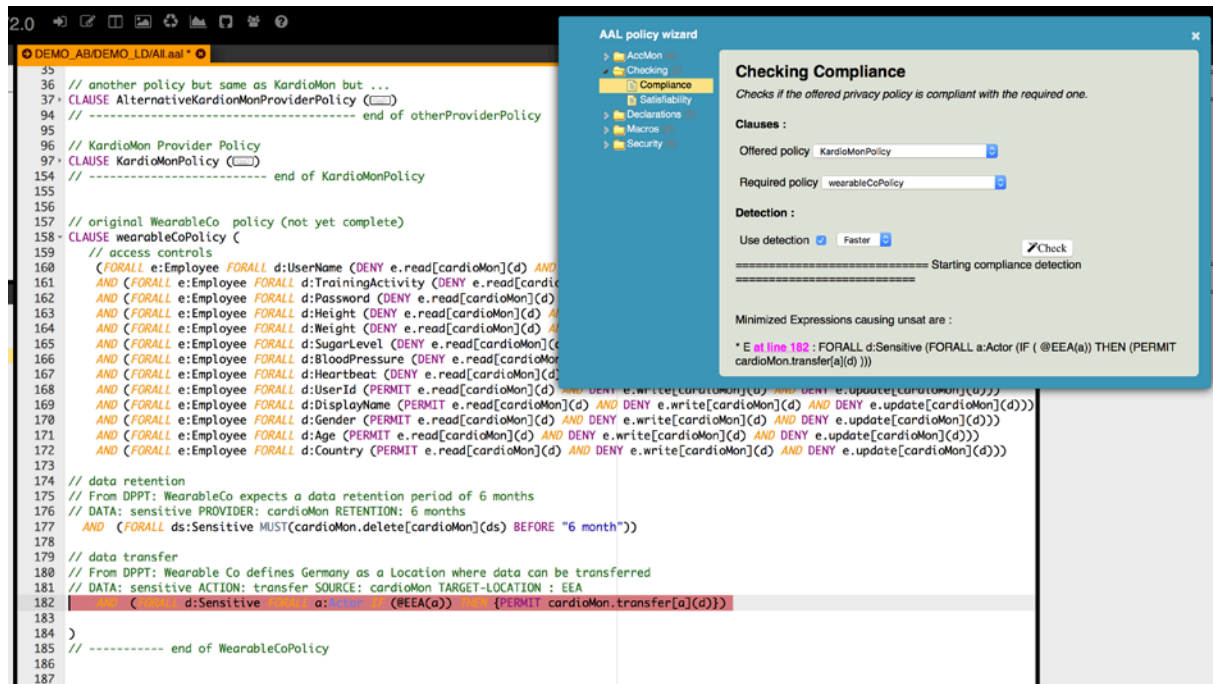


Figure 45: Demo scenario 2 – Localising policy conflicts in AccLab.

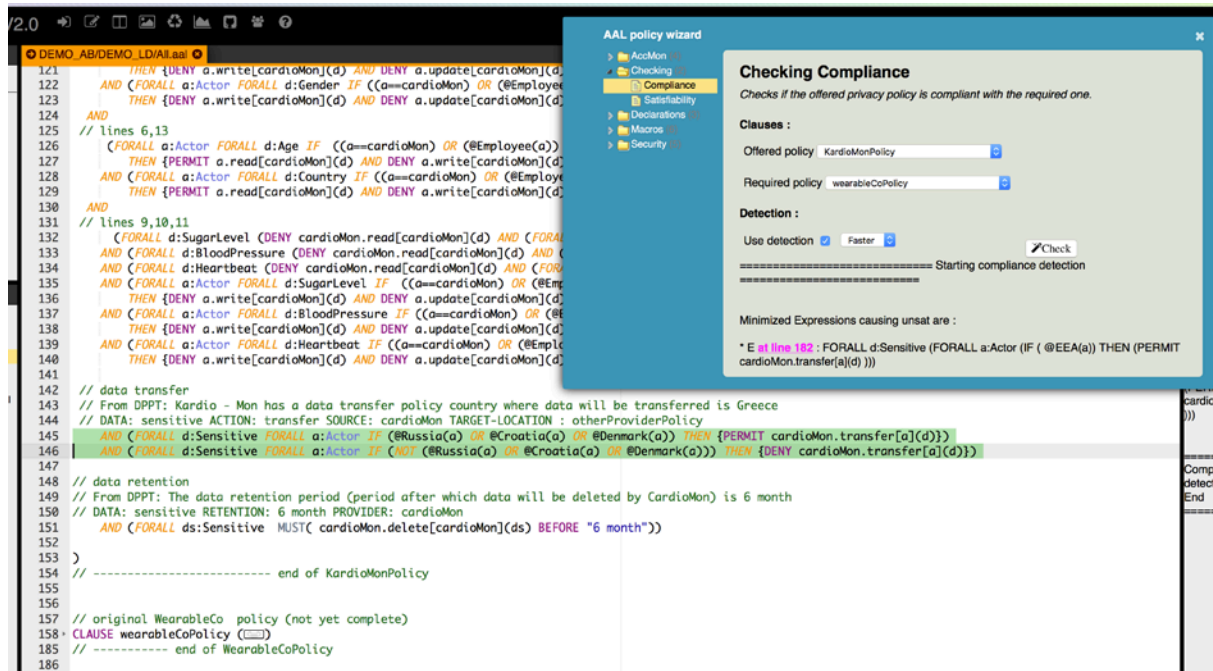


Figure 46: Demo scenario 2 – Example of conflict for data transfers in AccLab.

However, the selected choice is surely to browse the offers of Kardio-Mon and get an alternative proposal, may be more expensive, but compliant with EEA as target location. He found "AlternativeKardioMonProvidedPolicy" which enables transfers in all Europe, and he can prove with the tool that it is a compliant alternative with his requirement (see Figure 48). Once achieved, a business negotiation can start between the Wearable Co and Kardio-Mon.

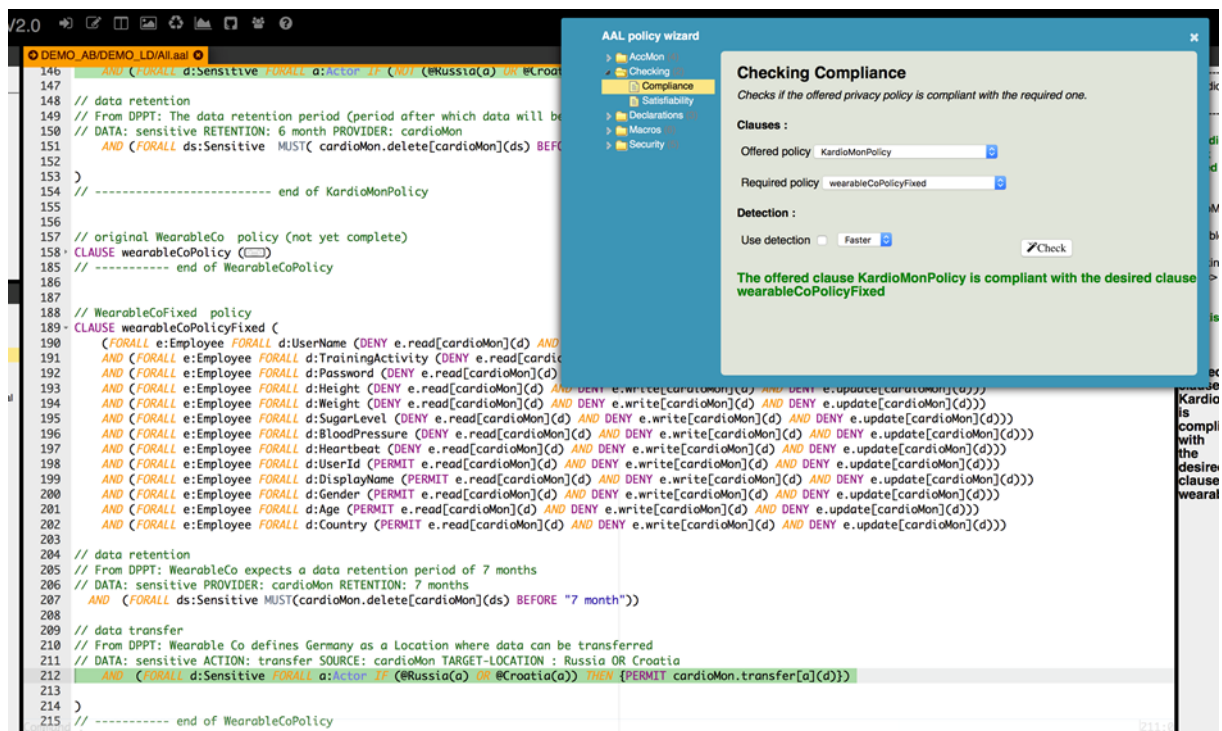


Figure 47: Demo scenario 2 – Correcting a conflict on data transfers in AccLab statements.

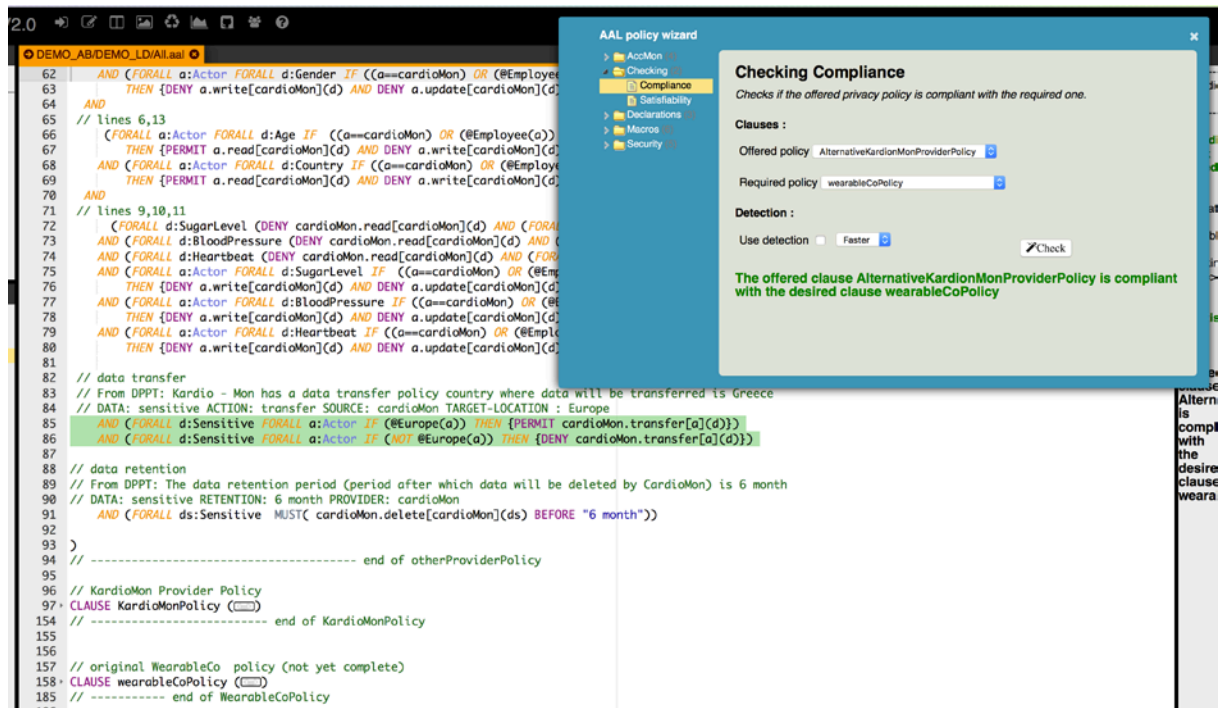


Figure 48: Demo scenario 2 – Checking an alternative policy offered by Kardio-Mon in AccLab.

When Wearable Service is chosen by the cloud customer Wearable Co, Kardio-Mon can proceed with the deployment of the policy file over the enforcement engine. This can be done by using the *Send to Engine* button (highlighted with a yellow rounded rectangle at the bottom of Figure 41). We can open that file just sent to see how the output generated by DPPT look like (see Figure 49). An example of policy representation output is included in Appendix.

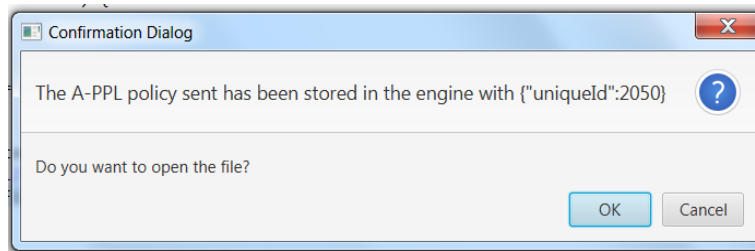


Figure 49: Demo scenario 2 - Confirmation Dialog about the policy being received by A-PPL Engine

5.3.7 Outcome

This scenario demonstrates how the privacy officer of a cloud provider like Kardio-Mon can use DPPT to define policies and a cloud customer like the Wearable Co can use AccLab to formalise their privacy and accountability requirements (in a formal but readable language, which is the Abstract Accountability Language) and compare them with the policy offered from Kardio-Mon (through a sophisticated editor and the interaction with an advanced logical prover). Once the policy specification process has been completed, Kardio-Mon can use DPPT to automatically generate the policy representation artefact, which is shown in Annex 9.1.2, and send it to the enforcement engine.

5.4 Demo Scenario 3: Incident Management

This scenario presents the perspective of the cloud environment to handle the exceptions detected automatically by the relevant tools and perceived by the actors involved in the operation of a complex cloud service chain.

5.4.1 Scope

This scenario aims to demonstrate the implementation of the accountability mechanisms in the cloud operational environment in order to handle incidents occurred in the cloud. The scenario introduces the A4Cloud monitoring tools, which collect logs from the cloud environment and analyse them, in order to raise incidents on potential policy violations. These tools can be the DTMT on the infrastructure layer or the AAS on the cloud service layer. The incident detection activates the incident handling process, which is supported by IMT. This is a tool targeted at organizations and teams, which handle computer security incidents, in practice any organization that provides or consumes an internet service. A problem experienced by incident handlers in the context of cloud computing, is the lack of access to sufficient incident information throughout the cloud provider chain.

5.4.2 Actors Involved

In this scenario, the IT administration and incident management and response teams are the primary actors. These actors are engaged in this scenario to operate the A4Cloud respective tools, which allow the detection of incidents and the management of the exception handling processes in order to mitigate any risks related to these incidents.

More specifically, the professional incident handlers and privacy officers of the cloud providers are involved in this scenario. Two cloud companies are participating in this scenario, namely DataSpacer, as the IaaS provider, and Kardio-Mon, as the SaaS provider. The Wearable Co privacy expert would not necessarily receive the needed information from Kardio-Mon. Furthermore, complicated cloud provider chains with multiple participants increase the need for more automated sharing of incident information, in which a particular level of automation for the response actions might be allowed.

5.4.3 Description of the demo scenario

This scenario refers to the monitoring and management of the runtime environment in order to detect and handle any anomalies, such as security breaches or policy violations, in the cloud. To this end, the scenario engages all the cloud providers in the wearables use case, who have a particular role in the collection and processing of the Wearable Co customers' personal data, and presents how the

responsible teams react in the detection of incidents happening in the environment. The detection of the incidents can be manual or automatic. This means that the scenario may cover the cases that: i) a tool deployed in the territory of a cloud provider identifies an anomaly in the normal operation of the cloud wearable service, and ii) the staff of the cloud provider dealing with the incident response process (the computer security incident response team – CSIRT) perceives that the behavior of the wearable service is not operating as expected and registers an incident.

Thus, the scenario involves the tools that can detect an incident and raise it to the respective IMT instance of the cloud provider. In detail and for the wearables use case, DTMT may detect an incident regarding a potential violation of the data transfer policy agreed between DataSpacer and Kardio-Mon. This incident is notified to the IMT instance of DataSpacer and depending on the assessment of the CSIRT of DataSpacer it can be communicated to Kardio-Mon, as well. On the other hand, the AAS instance of Kardio-Mon monitors the status of the Kardio-Mon VM and the DataSpacer infrastructure through the respective AAS clients and may detect incidents, such as incomplete data retention operations, due to the existence of backup versions of the personal data that should be deleted, or intrusion detection attempts. If so, AAS notifies the IMT instance of Kardio-Mon. Again the CSIRT of Kardio-Mon operates the respective IMT instance to assess the severity of the incidents received and handle in accordance to the policy.

The scenario flow is presented in Figure 50.

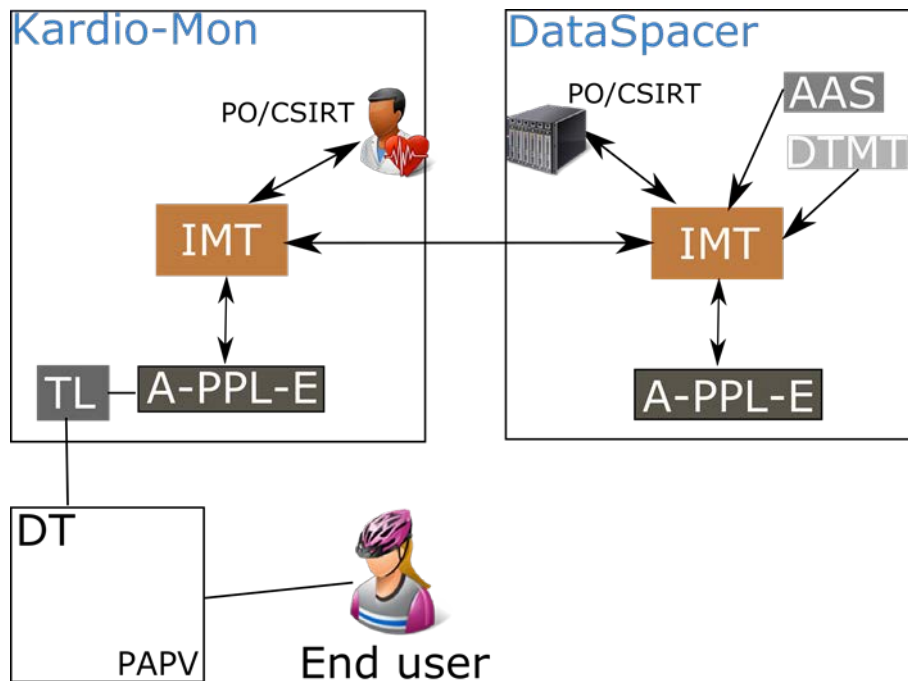


Figure 50: Demo scenario 3 – The flow of the incident management and communication processes.

As shown in Figure 50, IMT operates in the direct context of multiple tools from the A4Cloud toolkit, namely DTMT, AAS and A-PPLE. As explained above, IMT receives detected incidents from DTMT and AAS. When the CSIRT of Kardio-Mon decides that an incident should be notified to the Wearable Co customers, the IMT Kardio-Mon instance utilises A-PPLE and sends this notification through to A-PPLE. The latter registers the notification report to the TL of the target customer, so that it is retrieved from the respective DT. The DT instance of each customer is responsible for fetching the notification information from TL in order to inform the end user about the incident, through RRT (see demo scenario 5 and Section 5.6).

For the accomplishment of the demo scenario, we consider the case of an incident raised in the territory of DataSpacer, due to an unauthorised data transfer.

5.4.4 Addressing the Accountability Framework

This scenario sits on the heart of the operational and handle exceptions processes of the cloud accountability lifecycle. The scenario envisions the implementation of detective and corrective

accountability mechanisms, through addressing the functionalities required for the execution of the incident management and notification accountability support services. To this end, the scenario engages the machine logs and the notification accountability artefacts.

This scenario is based on the interactions shown in Figure 8 and Figure 9.

5.4.5 Prerequisites

The scenario assumes that the participating cloud providers are recruited with the appropriate skilled personnel to be able to make decisions on data protection issues both at an operational and a technical level. We, also, assume that this personnel has been exploited in the policy management and enforcement processes in demo scenario 2 (see Section 5.3) to accomplish the defined scenario steps (including the configuration of the IMT instances of both DataSpacer and Kardio-Mon) and that the wearable service is operating through the engagement of Wearable Co customers.

It must be noted that, the assigned DataSpacer personnel performs the following actions:

- The IMT instance of DataSpacer is configured with appropriate incident types – or incident categories – that Kardio-Mon are allowed to subscribe to. The tool is, also, configured with definitions of under which circumstances Kardio-Mon will be allowed to receive such incidents.
- The DTMT instance of DataSpacer is configured with the endpoint information of the IMT instance of DataSpacer.

Further to it, the assigned Kardio-Mon personnel performs the following actions:

- The IMT instance of Kardio-Mon is configured with appropriate incident types – or incident categories – in accordance to the ones defined for DataSpacer. The tool is, also, configured with the end point of the IMT instance of DataSpacer, as the provider of notifications. Finally, the IMT instance of Kardio-Mon subscribes the A-PPLE instance as the receiver of the notifications sent by this actor to either the Wearable Co or their customers.

The policy agreed between Kardio-Mon and DataSpacer indicates that the personal data of the Wearable Co customer collected and processed through the wearable service of Kardio-Mon should be maintained with the EEA. Following the deployment of the environment in Figure 15, a specific data volume (Storage Volume) is attached to the compute node, in which Kardio-Mon VM resides in, thus in the EU data center of DataSpacer.

5.4.6 Scenario Steps

The scenario is accomplished through the following steps:

- (1) The IT administrator of DataSpacer needs to respond to a hardware failure by migrating some of the data volumes attached to the EU compute node to another location. Thus, they access the OpenStack dashboard (see Figure 51) and detach Storage Volume from Compute Node 1, attaching it to Compute Node 2, which resides in US.
- (2) The DTMT instance of DataSpacer identifies this volume movement and logs it as a potential violation.

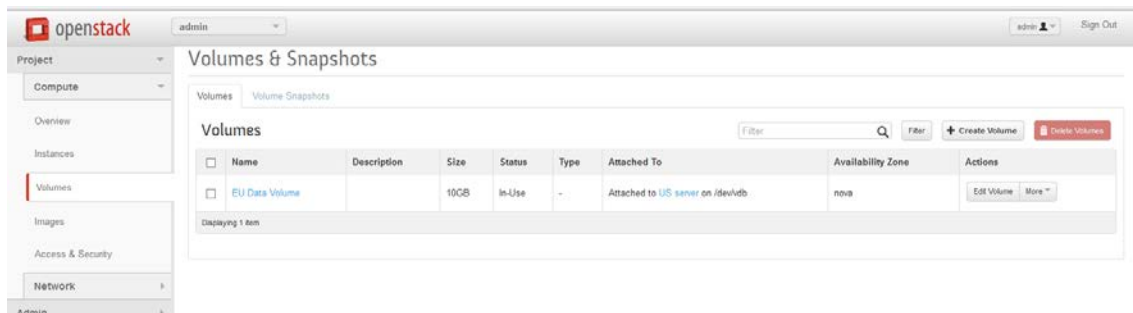


Figure 51: Demo scenario 3 - Attach-detach a data volume from a compute node.

- (3) The DTMT instance of DataSpacer notifies the respective IMT of DataSpacer.

- (4) The CSIRT of DataSpacer accesses IMT and browses through the received incidents through the menu on the left.
- (5) When accessing the incident list, the CSIRT of DataSpacer is presented with an overview of the current incidents, allowing them to see the summary, state, impact and type of each incident (see Figure 52).
- (6) By opening an incident, the CSIRT of DataSpacer is presented with further details (as shown in Figure 53), such as the origin of the incident, allowing them to know who provided the information about the status, impact, type, occurrence time, detection time, liaison, etc. Thus, the CSIRT know who to contact for further information. On the bottom, custom fields are shown. This is extra information that can be added based on the type of the incident. Attachments are for more complicated information, such as evidence or representation of incidents in a format friendlier to machines than humans, such as STIX or IODEF.

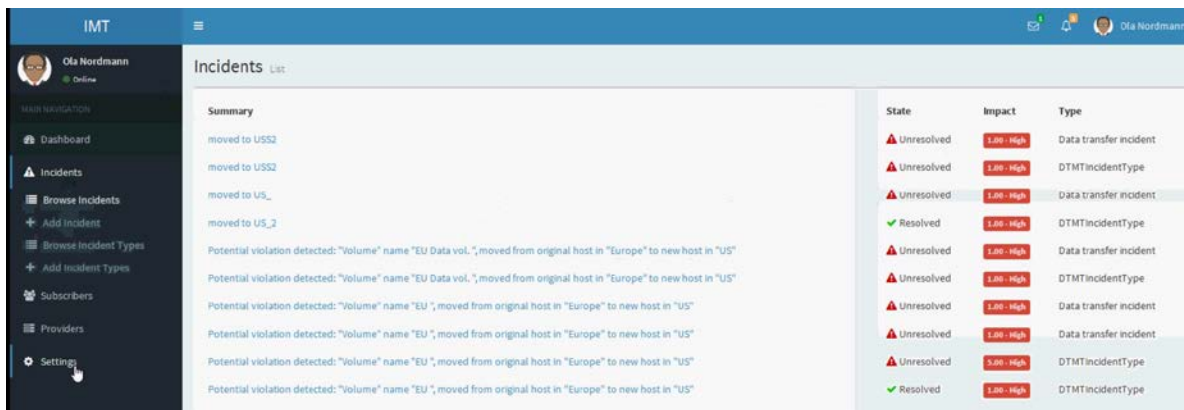


Figure 52: Demo scenario 3 - Browsing the incidents in the IMT of DataSpacer.

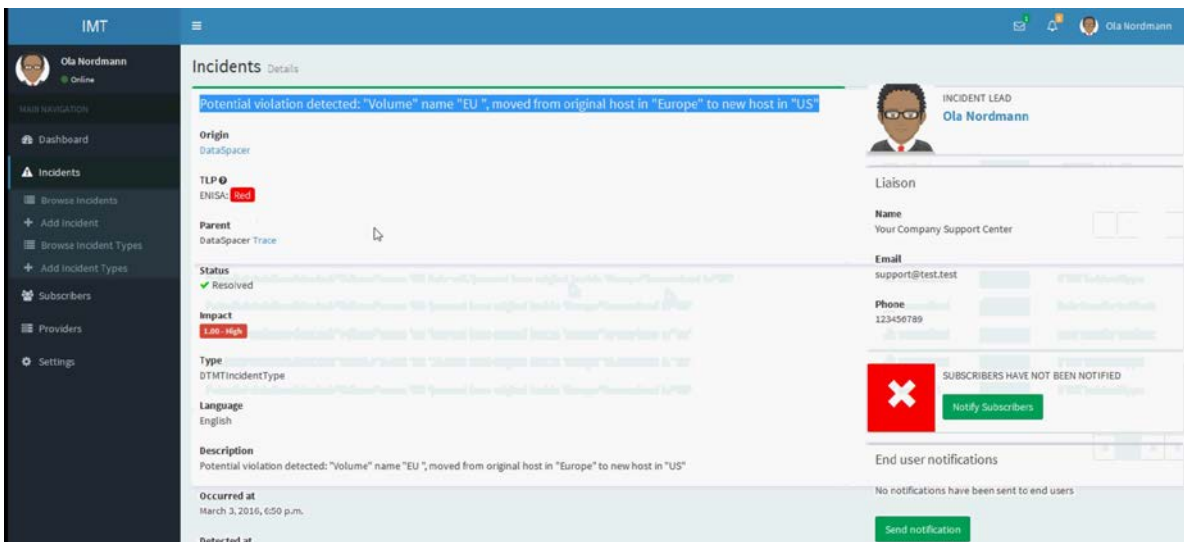


Figure 53: Demo scenario 3 - Browsing the details of a data transfer incident in the IMT of DataSpacer.

- (7) The bottom right area offers the CSIRT of DataSpacer the available actions at the current time of the incident status. If the incident has not been inserted by the CSIRT and originates from DTMT or AAS, then, a “derive incident” button is only visible. By pressing it, the CSIRT accepts the responsibility to undertake the management of this incident. The action creates a new incident record in the IMT instance of DataSpacer, based on the one being derived. This is to ensure the traceability of incidents, and make it more difficult to – by accident – forward information not intended for forwarding.
- (8) After having derived the incident, the CSIRT is allowed to update the incident details, if required, and notify the IMT subscribers, which in the case of DataSpacer is the IMT instance of Kardio-Mon.

The notification process is performed through the collaboration of the CSIRT and the privacy officer of DataSpacer and by clicking on the "Notify Subscribers" button in the incident details view.

- (9) Kardio-Mon is notified about the incident in their IMT instance. Any other incident coming from AAS can, also, be registered in the incidents' list of Kardio-Mon (see for example the creation of incidents through the AAS operations in Section 5.5). The respective UI is the same, like the one for DataSpacer in Figure 52.
- (10) The CSIRT of Kardio-Mon follows the same procedures in steps (4)-(8), as the respective team of DataSpacer, in order to accept the responsibility for managing the incident and further react to this incident in an accountable way.
- (11) The CSIRT and the privacy officer of Kardio-Mon assess the incident severity and type. Due to the fact that the incident relates to information that Kardio-Mon is handling on behalf of the Wearable Co, which is a non ICT SME. The latter do not have their own Computer Security Incident Response Team, but have bought this service from Kardio-Mon, as part of the Wearable Service offering.
- (12) The privacy officer of Kardio-Mon needs to decide if the Wearable Co is to be notified.
- (13) Through manual communication the privacy officer of Kardio-Mon and the privacy expert of the Wearable Co discuss whether to share this information with the end users or not.
- (14) If they decide to notify the Wearable Co customers, the privacy officer of Kardio-Mon presses the "Notify Subscribers" button in the incident details view and compiles the message to be communicated to them (see Figure 54).

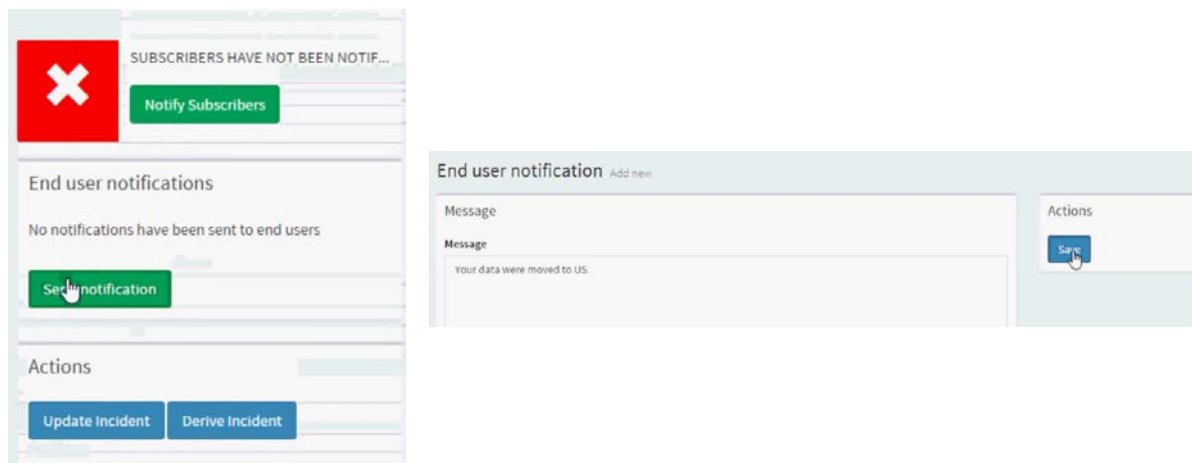


Figure 54: Demo scenario 3 – Notifying the end users through the IMT instance of Kardio-Mon.

By doing so, this demonstration scenario ends. In a logical order, the activities described in Section 5.6 about the incident notification and remediation should be followed by the Wearable Co customer.

5.4.7 Outcome

During this scenario, the different A4Cloud tools implementing detective (DTMT, AAS and TL) and corrective (IMT) mechanisms are interfacing with each other to detect incidents in the cloud environment, store evidence of how the incident is evolved in the cloud service supply chain and communicate incident information throughout the cloud provider chain and all the way down to the affected data subjects. As a result of this scenario in the wearable use case, a simplified incident format is produced and a simplified incident exchange process is deployed, which makes the solution usable for small companies (like Kardio-Mon and the Wearable Co), as well as large ones (like DataSpacer). Through this scenario, the cloud actors involved in the wearables use case are given support for maintaining traceability of the incidents and their way across the cloud service chain. Through the integration with the A4Cloud toolset, the incident management and response teams of the cloud providers are able to send notifications directly to the affected Wearable Co customers.

5.5 Demo Scenario 4: Monitoring and Audit

This scenario presents the perspective of the Auditor.

5.5.1 Scope

Evidence is often not readily available or accessible to auditors due to the fact that heterogeneous evidence sources are typically scattered across all of the architectural layers of the cloud. Also, auditing is often a manual process with little tool support and lacking automation. Furthermore, policy compliance is often not continuously asserted, but in large intervals. Cloud provider chains are often not considered in audits.

Through this demo scenario, we present AAS, as a service for automating the evidence collection and evaluation process. It enables automated auditing of multi-tenant and multi-layer cloud applications and infrastructures for compliance with accountability policies. Software agents are used for monitoring of potential evidence sources, collection of evidence, verification of policies against collected evidence, incident detection and reporting of policy violations.

5.5.2 Actors Involved

The primary actors involved in this scenario are the cloud auditors that conduct analysis of the cloud providers' compliance with data handling policies. Referring to the wearables use case the primary cloud actor(s) involved in this scenario is a third-party auditor that investigates the compliance of Kardio-Mon and Data-Spacer with data retention policies that are put in place by the Wearable Co.

5.5.3 Description of the demo scenario

In this scenario, an auditor is using AAS to automate evidence collection and evaluation on the basis of a data retention requirement that is defined in the accountability policy. Potential data retention violations are recognized in the service based on the existence of personal data in virtual machine snapshots at DataSpacer. Snapshots can violate data retention policies, if they hold personal data, for which the maximum retention time was exceeded. The personal data creation and deletion events produced by the A-PPLE instance of Kardio-Mon (see steps 1 and 3 in Figure 55) and the virtual machine snapshot events produced by the OpenStack environment in DataSpacer (see step 2 in Figure 55) are considered evidence. The collected evidence is used to detect snapshots that still hold personal data that should have been deleted.

A high level overview of the scenario interactions is presented in Figure 56.

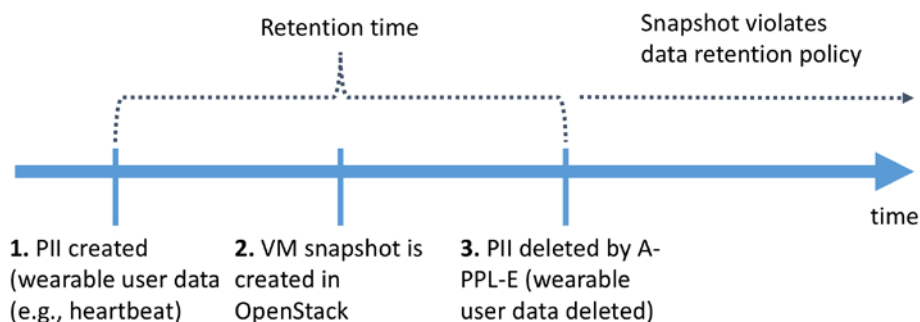


Figure 55: Demo scenario 4 - monitoring and audit scenario timeline

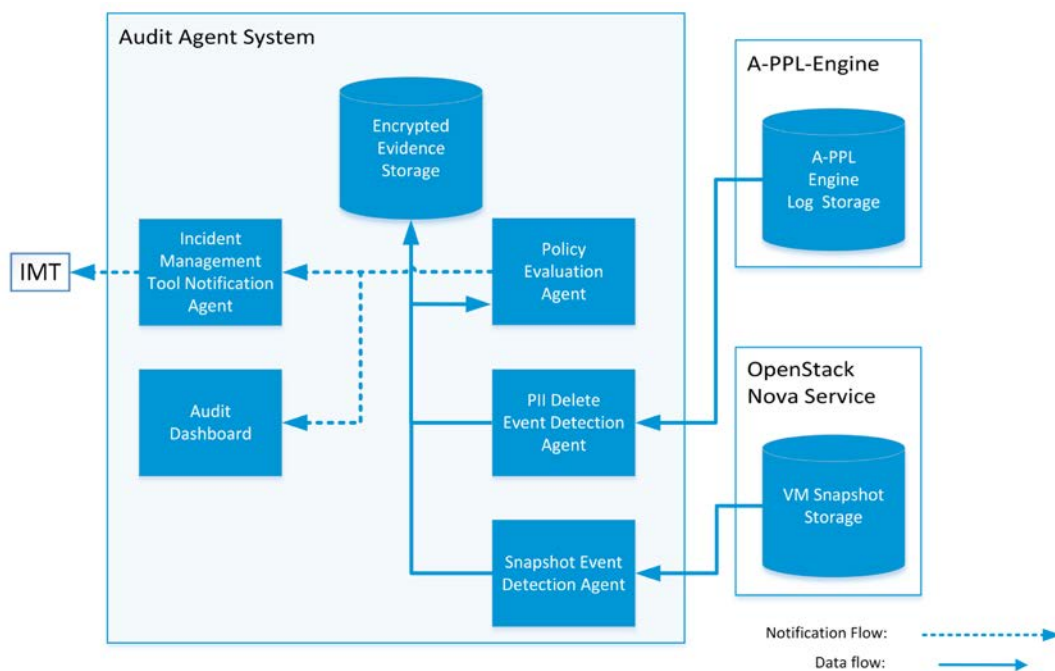


Figure 56: Demo scenario 4 - High-level Overview.

5.5.4 Addressing the Accountability Framework

AAS supports continuous monitoring, which is the basis for incident detection that triggers the exception handling phase of the lifecycle for accountability, as well as the protection of evidence that is produced in the operational phase. AAS is therefore part of the detective mechanisms used in the accountability framework. Furthermore, AAS enables automated internal and external audits in the audit and validation phase.

This scenario is based on the interactions shown in Figure 6, Figure 7 and Figure 12.

5.5.5 Prerequisites

In order for AAS to collect evidence and allow auditing, it must be explicitly instructed to do so. To limit the scope of evidence collection to only what is essential to fulfil its task (this is essential from a data protection perspective), the evidence collection is always based on an accountability policy (expressed in A-PPL format). Therefore, AAS depends on policy definitions being completed and available as an A-PPL accountability artefact, produced, as explained in Section 5.3. Additionally, AAS works most effectively, when all cloud providers (i.e., Cardio-Mon, Map-on-Web and Data-Spacer) run their own instance of AAS. Although this is not a hard requirement, AAS works best in such a scenario, which is why in this scenario Cardio-Mon and DataSpacer are assumed to run separate AAS instances.

5.5.6 Scenario Steps

This demonstration scenario is executed through the following steps:

- (15) The auditor launches the AAS instance provided by Kardio-Mon and is presented with an overview of currently active auditing and monitoring tasks, as shown in Figure 57.



Figure 57: Demo scenario 4 - AAS dashboard overview.

- (16) The auditor configures an audit task based on A-PPL policy that is in effect by parsing the XML document, and extracting the relevant rule and its attributes, as seen in the code snippet in Figure 58.

```
<ob: Obl i gat i on el ement I d="a- ppl _r ul e_3">
  <ob: Tr i gger sSet >
    <ob: Tr i gger At Ti me>
      <ob: St ar t >
        <ob: St ar t Now / >
      </ ob: St ar t >
      <ob: Max Del ay>
        <ob: Dur at i on>P0Y6M0DT0H0M0S</ ob: Dur at i on>
      </ ob: Max Del ay>
    </ ob: Tr i gger At Ti me>
  </ ob: Tr i gger sSet >
  <ob: Act i on Del et e Per sonal Dat a / >
</ ob: Obl i gat i on>
```

Figure 58: Demo scenario 4 - Data retention obligation in A-PPL.

- (17) When the auditor has added all parameters that are not extractable directly from the policy (i.e., audit interval, agent runtime environment and virtual machine name), the audit task is deployed (see Figure 59 for the complete scenario configuration).

Now, evidence is continuously collected and the combination of DataSpacer's snapshot events and Kardio-Mon's A-PPLE events is continuously audited. All relevant events are securely recorded as evidence records in AAS. An evidence record that originates from A-PPL-E's operation logs looks like the one in Appendix 9.3.1, while an evidence record that originated from OpenStack's Nova service looks like the one in Appendix 9.3.2.

- (18) Violations are presented to the auditor and automatically forwarded to Kardio-Mon's IMT for further processing (see Figure 60 for the visual representation of the violation in AAS).

Audit Agent System

[Audit overview](#)
[Create audit](#)
[Results](#)
[Records](#)

Create audit

Data Handling
Access control
Custom

Data handling policies

Data retention policy

Data location policy

Policy 2

☒ Extract from policy

Tasks

☐ Snapshot check

☒ Data Retention Audit Task

This audit task recognizes potential data retention violations based on the existence of PII in virtual machine snapshots

[Edit](#)

Configuration

1. Audit type*

Periodic

2. Container*

Main-Container

3. Check interval:*

1

4. VM name:*

Kardio-Mon-PII-Store

5. Data Retention PII Subject:*

Panos

6. Open Stack container:*

DataSpacer

[save](#)

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

[Delete](#)
[Execute](#)

Figure 59: Demo scenario 4 - AAS audit task creation view.

Audit Agent System

[Audit overview](#)
[Create audit](#)
[Results](#)
[Records](#)

Results

Violation (1)
Need Review (0)
Passed (0)

[Refresh](#)

Filter results

☐ Policy ID

All results

☐ Timeframe

2015-12-09 00:00 - 2015-12-09 23:59

[filter results](#)

2015-12-09T10:33
data retention violation
data retention policy
data retention check

This audit task recognizes potential data retention violations based on the existence of PII in virtual machine snapshots

Evidence

ActionID:
 PII Data Retention Violation - Snapshots of PII Store(Kardio-Mon-PII-Store) available between 2015-12-09 10:29:41.0 and 2015-12-09 10:31:43.0 (contains PII of Panos)@Main-Container(10.0.0.6)

ActorID: DataRetentionPolicyEvaluationAgent_1042_Main-Container

Policy reference: 1042

Acting tool: DataRetentionUsagePII

Detection time: 2015-12-09T10:33:03.82

Occurance time: N/A

Record Reference: 0

Figure 60: Demo scenario 4 - AAS policy violation presentation in the AAS dashboard.

5.5.7 Outcome

The outcome of this scenario is a continuous monitoring of the services provided by Kardio-Mon and DataSpacer, as well as a continuous audit of the collected evidence to detect data retention policy violations. The absence of a violation thereby indicates compliance with the data retention requirements stated in the A-PPL policy that applies to this scenario. If a data retention violation is detected, this incident is reported to the IMT for further handling (see the respective scenario in Section 5.4).

5.6 Demo Scenario 5: Data Subject Controls

The scenario presents the perspective of the Wearable Co customers, as data subjects.

5.6.1 Scope

The scope of this demonstration scenario is to showcase the capabilities of the data subjects in exercising their right for controlling the way that their personal data is handled in the cloud. As such, in this scenario, we introduce the data subject enablement tools, namely DT and TL, which are used in the wearables use case by the Wearable Co customers to get information about any disclosures occurred in their personal data shared with Kardio-Mon and the rest of the cloud chain. In this scenario, we, also present how the data subjects, the Wearable Co customers in the wearables use case, can be notified of any incidents happened in the cloud that affect the privacy of their data, and undertake remediation actions to mitigate the risks stemming from such data disclosures.

5.6.2 Actors Involved

The Wearable Co customer is the primary role of this scenario, which may, also, involve Kardio-Mon and the Cloud Auditor, as recipients of the requests raised by the customer.

5.6.3 Description of the demo scenario

In this scenario, we assume that an individual (a Wearable Co customer) acquires a wearable device, sold by the Wearable Co, and wants to register to the online application that is offered to her in order to manage the data collected from the device. The individual accesses the Web front end of the wearable service application and registers into it, by reading the policy offered to her by the Wearable Co for using the cloud service operated by Kardio-Mon and giving her consent for the policy rules. Once the individual gets an account to the cloud application, she enters it and accesses the provided functionalities. The individual as the Wearable Co customer has downloaded and installed DT, which allows browsing through her personal data disclosures with all the cloud providers. At some point in time, she gets a new notification on the respective widget of the DT UI. By pressing this notification, RRT loads and presents her information about an incident occurred in the cloud service chain of Kardio-Mon. The Wearable Co customer wants to react on this and she searches RRT for proposed remediation actions. By reading through them, she decides which action to adopt.

5.6.4 Addressing the Accountability Framework

This scenario refers to the validation and handling exception phases of the lifecycle for accountability. The tools introduced in this scenario are developed to address detective and corrective accountability mechanisms and implement the remediation and the validation accountability support services. More specifically, the use of DT (through TL for a secure communication with the tools deployed in Kardio-Mon) addresses the validation functionalities of the Wearable Co customer to detect any unauthorised disclosures occurred in their personal data shared with the various cloud service providers, including Kardio-Mon. The invocation of RRT happens during the implementation of the remediation service, when a Wearable Co customers receives notifications on policy violations occurred in the cloud environment affecting their privacy. In this case, RRT supports the customers in accessing potential remedies.

This scenario is based on the interactions shown in Figure 13 and Figure 11Figure 3.

5.6.5 Prerequisites

The scenario evolves in various times of the operational phase of the wearable use case. In all the cases, the execution of the scenario implies that the Wearable Co customer has registered into the Wearable service application (by giving consent to the policy rules) and allowed the wearable cloud service instance of Kardio-Mon to collect personal data. Moreover, since this scenario addresses the implementation of the remediation accountability support service from the perspective of the Wearable Co customer, we assume that an incident of any type has been raised in the cloud environment (as per the demo scenario 3 in Section 5.4) and the incident has been sent from Kardio-Mon IMT instance to A-PPLE, so that it is communicated to the end users.

5.6.6 The scenario steps

The scenario is accomplished through the following steps:

- (1) The Wearable Co customer downloads and installs DT in their device.
- (2) By opening the DT application in a Web browser, the customer gets the view of Figure 61. This is the front end of the DT tool, which allows tracing the disclosures of personal data with the cloud providers in a trace or a timeline view.

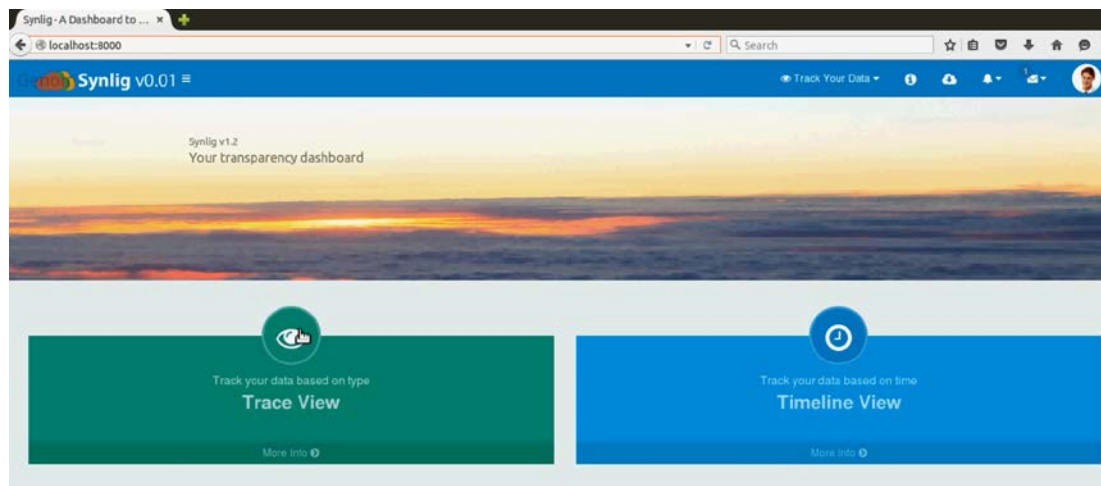


Figure 61: Demo Scenario 5 – Accessing DT.

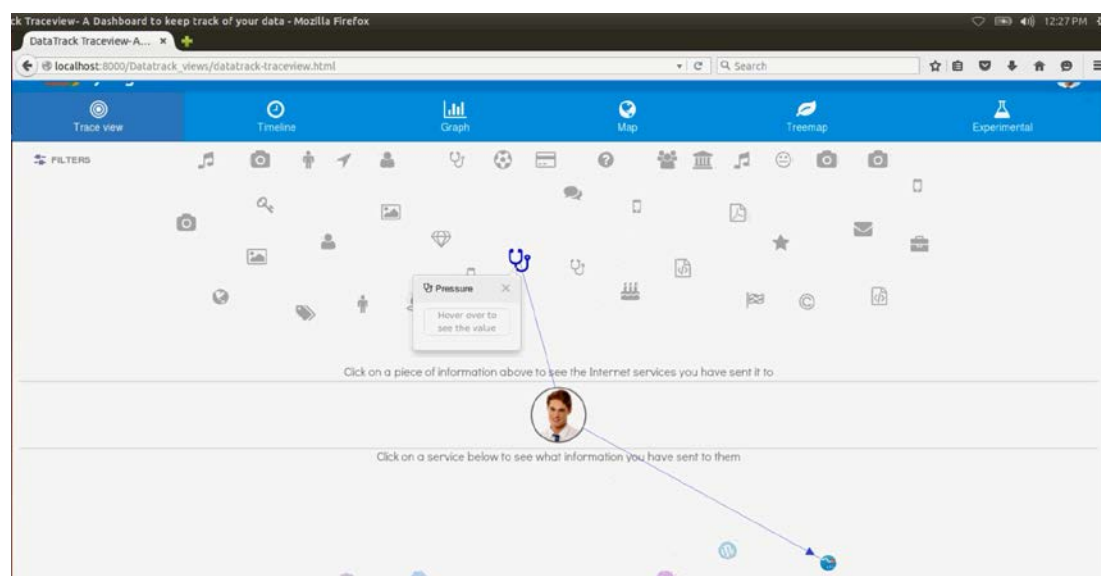


Figure 62: Demo Scenario 5 – The trace view of the DT tool.

- (3) The Wearable Co customer clicks to load the trace view (see Figure 62).

- (4) The customer selects the icon of a cloud provider to trace the personal data associated with the disclosure to this provider (see Figure 62).
- (5) The customer can also select the icon of a personal data attribute and trace which cloud providers maintain this data and with which value.
- (6) Then, the Wearable Co customer decides to join the wearable service application, as per the operations in Appendix 9.2.1.
- (7) By the time that, the customer registers into the application (see Figure 79), the local instance of DT is notified of the link of the customer with Kardio-Mon.
- (8) The Wearable Co customer refreshes the trace view of DT and can see the Kardio-Mon icon on the providers' panel (see Figure 63).
- (9) The customer clicks on the Kardio-Mon icon and gets a visualisation of the personal data disclosed to this cloud provider. For each of this data, the customer can view the latest value attribute to each type of the personal data.

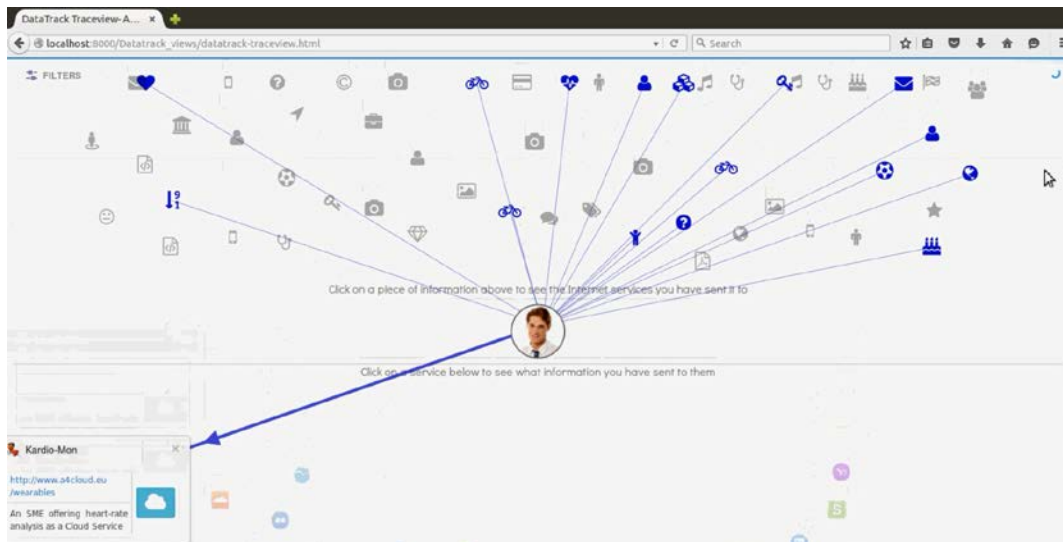


Figure 63: Demo Scenario 5 – Connecting Kardio-Mon with DT.

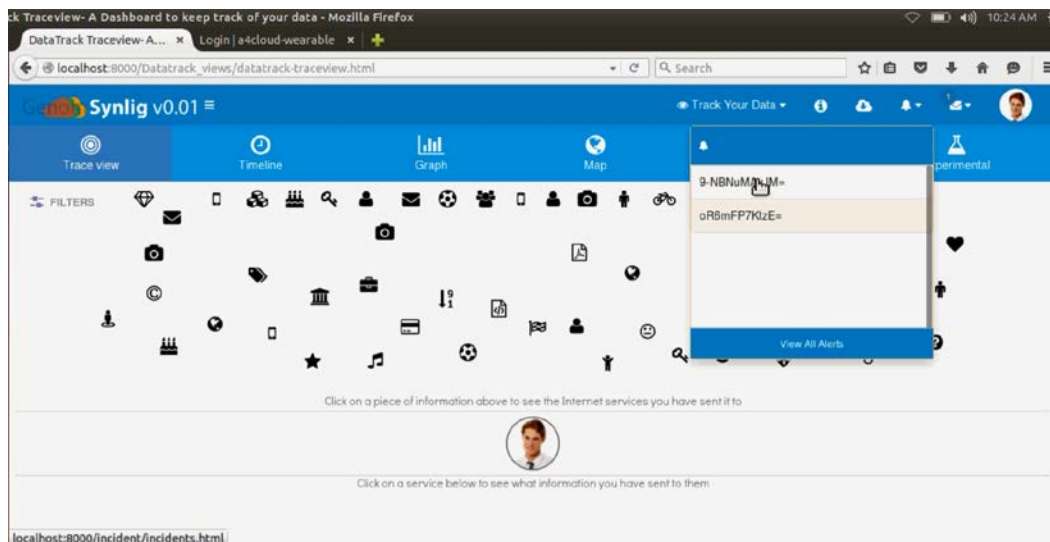


Figure 64: Demo Scenario 5 – Receiving a notification on the RRT widget of DT.

- (10) In a point in time, the Wearable Co customer receives a new notification in the RRT widget of DT (see Figure 64).

- (11) By clicking the notification, RRT UI loads, as shown in Figure 65. The UI splits into three views, namely, the upper left view for the list of received notifications, the upper right view with the details of a received notification, and the bottom view, listing the proposed remediation actions for an incident reflected in a notification.
- (12) The Wearable Co customer selects a notification and browses through the incident details.
- (13) The customer decides to show the remedies proposed for this notification, by clicking the respective button (see Figure 66).
- (14) By browsing the recommended actions in Figure 66, the customer decides which one to apply.

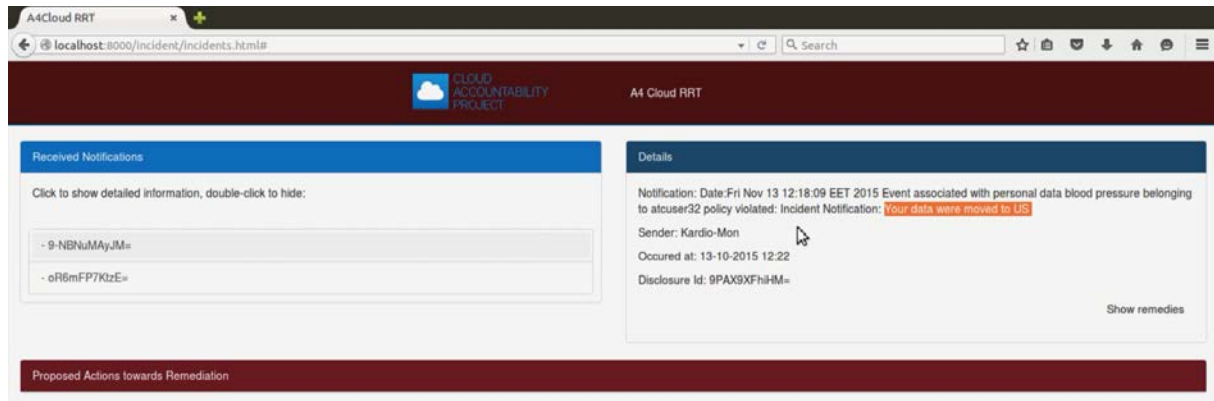


Figure 65: Demo Scenario 5 – Accessing RRT.

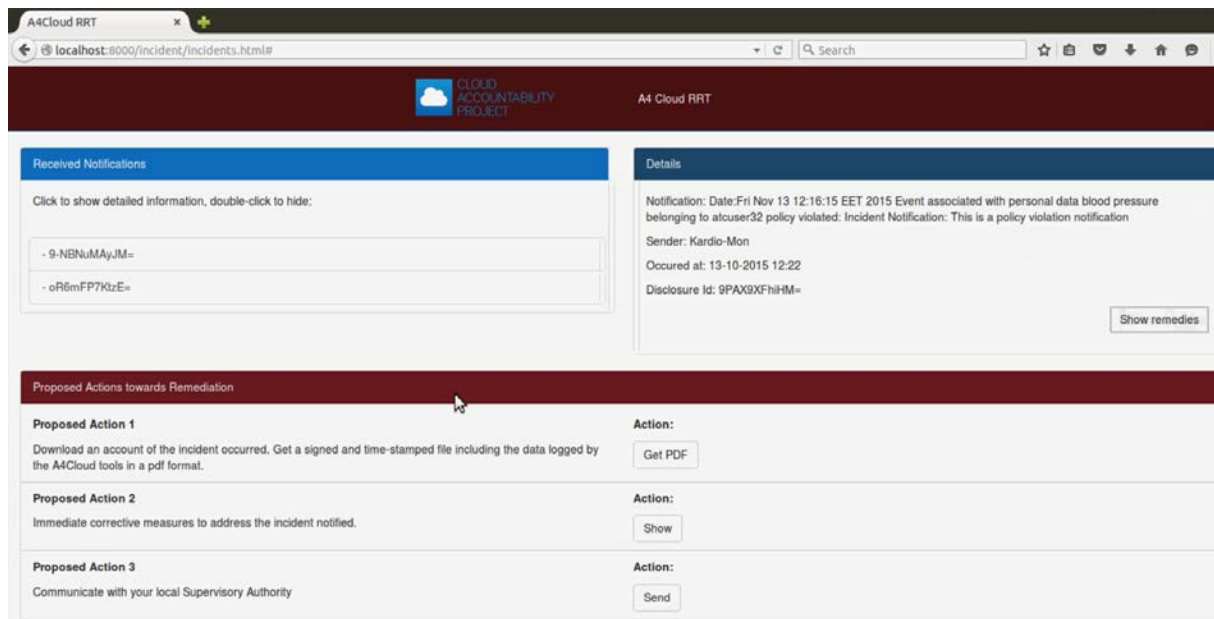


Figure 66: Demo Scenario 5 – Viewing the remediation options for a received notification in RRT.

5.6.7 Outcome

As a result of the actions performed in this scenario, a set of recommendations for the Wearable Co customer has been issued through the RRT view. These recommendations consult the customer in responding to a potential notification on an incident occurred in the cloud. Further to these recommendations, the customer may apply specific redress actions.

6 Supporting the Provision of the Account

This section points out the role of evidence in the provision of the account, hence supporting assurance and trustworthiness. In particular, it recalls the concept of accountability which highlights the responsibilities of an organisation in order to be accountable [4]. This is central to the concept of accountability [5]: *“Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly”*. Underpinning the concept of accountability is the provision of an account, which involves the gathering of evidence supporting organisational practices. This section then discusses the problem of assurance in a sample cloud supply chain. This discussion helps clarifying the requirements for supporting security and privacy assurance in cloud ecosystems.

6.1 Evidence-Based Accountability

The Cloud Accountability Project points out the need for evidence-based accountability in order to support the assessment of whether adopted security and privacy solutions (e.g. technologies, processes, etc.) are suitable for the specific cloud ecosystems, and hence provide assurance [4]. Cloud ecosystems involve various actors with different responsibilities. Emergent relationships among cloud actors give rise to the need for chains of evidence – *“A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control and possession of the evidence”* [5] – and evidence in terms of organisational practices. On the one hand, it is necessary to validate gathered evidence and trace its source. On the other hand, evidence (is transformed and) propagates across system and organisational boundaries. From a technical viewpoint, evidence is considered among the three fundamental capabilities of an accountable system [6]:

- **Validation:** “It allows users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected”
- **Attribution:** “In case of a deviation from the expected behaviour (fault), it reveals which component is responsible”
- **Evidence:** “It produces evidence that can be used to convince a third party that a fault has or has not occurred”.

Therefore, gathering evidence has a critical role in supporting assurance – *“Assurance is about providing confidence to stakeholders that the qualities of service and stewardship with which they are concerned are being managed and maintained appropriately”* [7]. This is also particularly important while dealing with emergent threats [8] due to a certain extent to the shift required while deploying new technological paradigms like cloud computing.

6.2 Assurance of Cloud Supply Chain

Figure 67 shows a sample supply chain involving different actors: a cloud customer and two cloud service providers. The emergent relationships among actors form cloud supply chains defined in terms of cloud roles [4]. From a data protection perspective [9], cloud actors also have different roles and responsibilities (i.e. data subject, data controller, and data processor). The cloud supply chain generalise the cloud actors and roles that are involved in the demonstrator scenario. It is challenging to support operational compliance to policies and regulations. Security and privacy depend on the operational effectiveness and appropriateness of deployed controls and their dependencies. It is desirable to build and maintain dynamic assurance cases of security and privacy controls (providing security and privacy assurance of the cloud supply chain through continuous monitoring). The following points characterise some aspects of assurance in cloud supply chains (Figure 67):

1. Different security and privacy controls are deployed across a cloud supply chain.
2. It is challenging to provide transparency and assurance to cloud customers.
3. It is necessary to provide technological solutions to support continuous assurance.

4. Operational evidence of security and privacy controls is required to provide assurance (such evidence can also support certification).

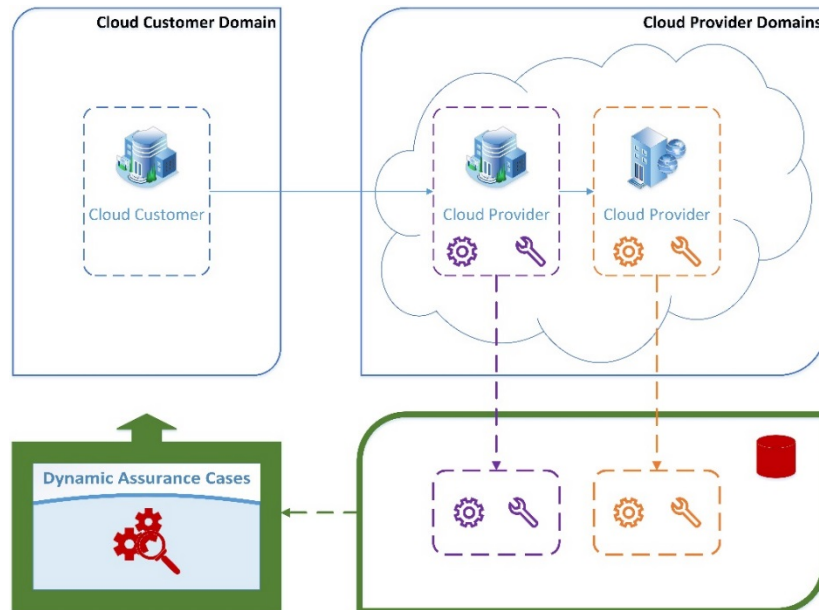


Figure 67: Assurance in a cloud supply chain

Throughout the cloud supply chain, cloud actors share the overall responsibility of security and privacy. These objectives are achieved and supported by adopting and deploying different security and privacy technologies (as depicted in Figure 67). Such technologies provide different support within and across cloud actors' domains. The problem then is how to provide assurance that the adopted technologies as a whole support security and privacy objectives across the supply chain, that is, how to provide supporting evidence that the adopted security and privacy technologies are appropriate and effective for the specific cloud supply chain.

6.3 Structuring the Provision of the Account

The Cloud Accountability Project has developed diverse mechanisms supporting accountability. Different mechanisms support cloud actors to be accountability at different stages (i.e. preventive, detective and corrective) orchestrated by the accountability reference architecture and lifecycle. The problem then is how to support the provision of the account in order to ease an operational understanding of accountability. We have addressed this problem by structuring the provision of the account in order to link accountability to the evidence supporting it as a whole. This underpins accountability to the mechanisms and associated evidence supporting it. Figure 68 shows the assurance structure supporting the provision of the account.

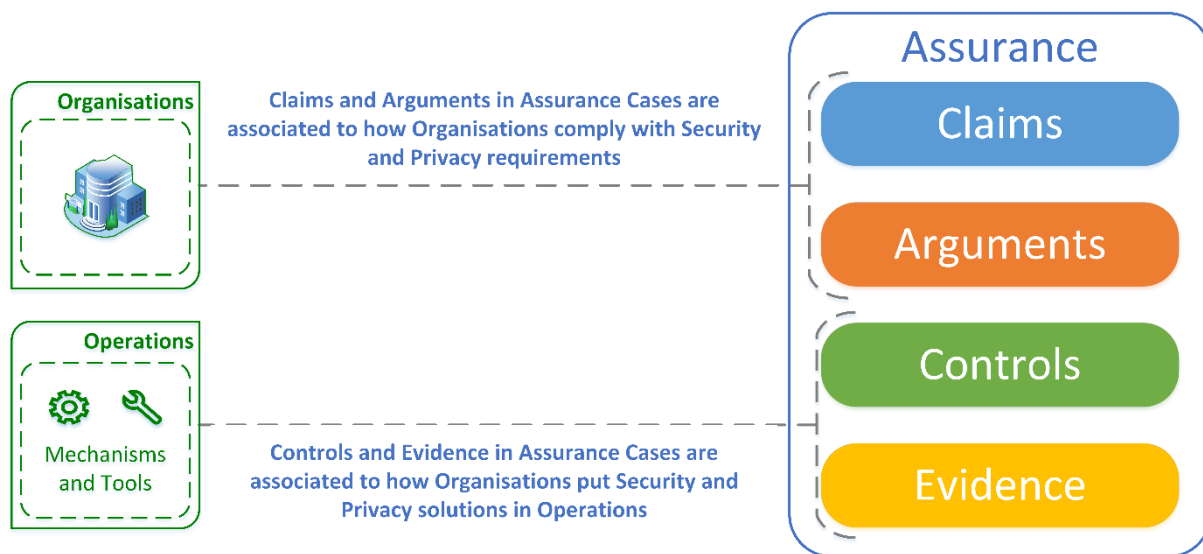


Figure 68: Structuring the provision of the account.

The assurance structure consists of high level claims that are usually associated with organisational objectives or expected behaviours of cloud services. Assurance claims can be refined in terms of arguments, which are expected to be valid and true in order to support the top level claims. Such arguments can take into account various organisational information, such as organisational practices, compliance to standards, best practices and guidelines. These relationships between claims and arguments can capture aspects of accountability, as expressed in the accountability definition and model. For example, an organisation can make specific claims associated to accountability attributes that are then supported by specific arguments associated to accountability practices. Further refining the structured assurance supporting the provision of the account is necessary to support any argument, hence any claim, by specific (accountability, security and privacy) controls and associated evidence in operational environments. Similarly, such controls and associated evidence take into account also the accountability mechanisms. The relationships between claims, arguments, controls and evidence form an assurance structure, linking organisational objectives with operational ones, supporting the provision of the account for cloud supply chains.

6.3.1 Evidence of Cloud Controls

This section discusses various aspects of implementing assurance in cloud supply chains, that is, emerging technical considerations to be addressed while implementing a system supporting assurance. System functionalities that support assurance for the whole cloud supply chain are discussed. Notice that specific technical points are not implementation steps to follow, but rather insights which inform how a structured assurance captures the demonstrator scenario. Cloud service providers often work together (e.g. sub-contract services or relies on third-party resources constrained by specific service level agreements) in order to provide specific services to cloud customers. This may result in complex cloud supply chains involving several cloud service providers working jointly. In a cloud supply chain, security is therefore a shared responsibility among the actors involved. Cloud providers deploy different security and privacy controls in order to guarantee critical service features. In order to support accountability, cloud providers need to gather evidence as proof that security and privacy controls are effective and suitable in addressing emerging threats. Cloud providers can then be entrusted with sensitive data. Table 4, for example, lists some controls drawn from the CSA Cloud Control Matrix [10], in particular, controls from two different domains: *Data Security & Information Lifecycle Management*, and *Supply Chain Management, Transparency, and Accountability*. Similarly, the NIST Cloud Computing Security Reference Architecture identifies a list of controls (requirements) to mitigate security risks [11].

Table 4: Examples of controls from the CSA Cloud Control Matrix.

Control Domain	CCM	V3.0	Updated Control Specification
	Control ID		

Data Security & Information Lifecycle Management: Classification	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.
Data Security & Information Lifecycle Management: Handling / Labeling / Security Policy	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
Data Security & Information Lifecycle Management: Ownership / Stewardship	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.
Supply Chain Management, Transparency and Accountability: Supply Chain Metrics	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.

However, both NIST and CSA aim mitigating security risks from a high-level perspective, providing no guidelines on which operational aspects of controls should be supervised and which data should be stored in order to prove that deployed controls are effective and suitable in addressing emerging threats. Therefore, a specific set of controls and associated (type of) evidence should be defined for each specific cloud environment. However, independently of any cloud environment, it is possible to build a general framework that will ease the task of managing these controls and evidence. It is necessary that each security and privacy control clearly defines which (type of) evidence it requires to be gathered in a cloud supply chain. Evidence should focus on operational aspects of deployed controls that need to be monitored. If such evidence is not produced, controls cannot be regarded as supporting security and privacy objectives (e.g. in terms of compliance with security and privacy policies). The proposed CloudTrust Protocol (CTP), for example, provides a basic mechanism for sharing evidence across cloud supply chains [12], hence supporting transparency in the cloud.

6.3.2 Linking Controls to Supporting Evidence

As discussed in the previous section, it is necessary to associate controls to evidence about them. This section provides a brief rationale of how controls are associated to (or supported by) evidence, the framework of evidence provides further discussion and a detailed model underlying the gathering of evidence [13]. Such evidence can be gathered in a dedicated storage platform (e.g. a software defined storage). Within the dedicated evidence storage, it is necessary to establish and maintain (e.g. creating, reading and updating) relationships between controls and associated evidence. Each *Control* may have different types of Evidence Items associated with it. Note that the same type of Control may be configured differently in operation, hence, it may be necessary to store different types of evidence. A *Control* will be described by (at least) three fields, as listed by the CSA Cloud Control Matrix: ID, control domain and description. Each Control should be supported by at least one Evidence Item. This evidence will support auditing of the Control (e.g. in terms of policy compliance). Each Control should keep track of its associated Evidence Items. It can also include user-defined metadata (e.g. what type of evidence it is associated with, timestamps like when was the last time this control was audited, etc.). Finally, an *Evidence* is a collection of information that needs to be kept for a Control to support auditing. It can be regarded as a wrapper for the required information. Its contents are, a priori, not of interest for the Control Manager. On the contrary, they will be necessary for an auditor to grant that the deployed set of controls is suitable and effective in order to mitigate security and privacy threats. As with Controls, an

Evidence Item may include user-defined metadata (e.g. type of evidence stored such as log file, configuration file, performance metrics, who generated it).

6.3.3 Roles in Providing Assurance

A cloud supply chain will need to meet certain controls to prove its accountability. These controls require evidence as proof of their fulfilment. As it was mentioned previously, it is necessary that there exists some permanent storage platform in the cloud supply chain where this evidence will be stored. This responsibility will be assigned to one cloud provider. This storage platform should be accessible by the other providers in the cloud supply chain, as this is where they will store their Evidence Items. It should count with the required security measures to guarantee confidentiality, integrity, and availability (e.g. access control, encryption, backups, etc.). Figure 69 shows a sample cloud supply chain in terms of actors and their associated responsibilities in sharing and contributing to an evidence storage for controls.

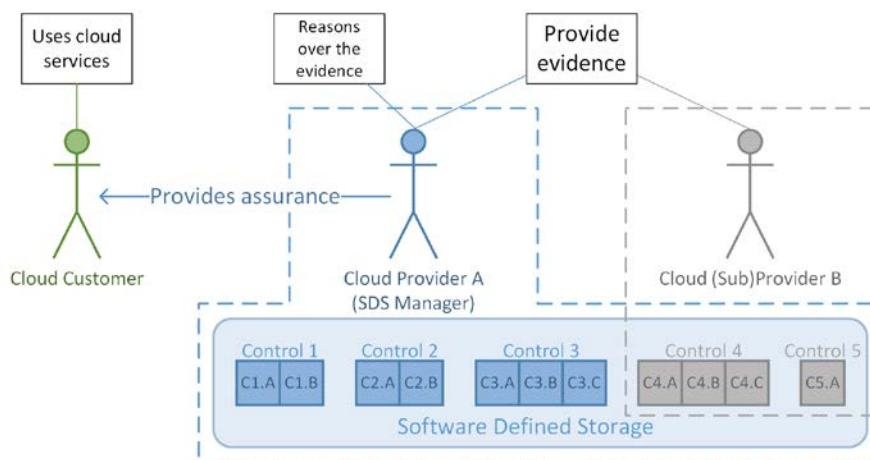


Figure 69: Sample cloud supply chain.

In this example, different controls (numbered 1 to 5) are deployed to guarantee security and privacy of data. The evidence associated with them is stored in specific locations which are managed according to the responsibilities in the cloud supply chain. In this example, Cloud Provider A is in charge of managing a software defined storage platform, as well as it is responsible for providing the evidence for controls 1, 2, and 3. On the other hand, Cloud Provider B (subprovider) is only responsible for providing the evidence for controls 4 and 5, which are the ones that affect it. Once that all the evidence is produced, Cloud Provider A is able to reason over it and, if everything is correct, eventually demonstrate to the Cloud Customer that all the controls are implemented adequately, hence providing assurance.

6.3.4 Evidence Access

As depicted in the previous section, specific Evidence Items are to be provided by specific cloud providers. The access to this evidence should be limited only to the providers who are responsible for them (and, when appropriate, to the auditors). A Control may require several Evidence Items in order to be considered complied with. These Evidence Items could be supplied by different cloud providers. In this case, it would be desirable that each provider is only allowed access to its related Evidence Items and no others, hence preventing them from being tampered with by unrelated providers. This scenario is shown in Figure 70, where Control B requires evidence coming from two different sources. Evidence Items 4 and 5 should only be accessed by Cloud Provider A and Evidence Item 6 only by Cloud Provider B. In this case, an object-level access control is required.

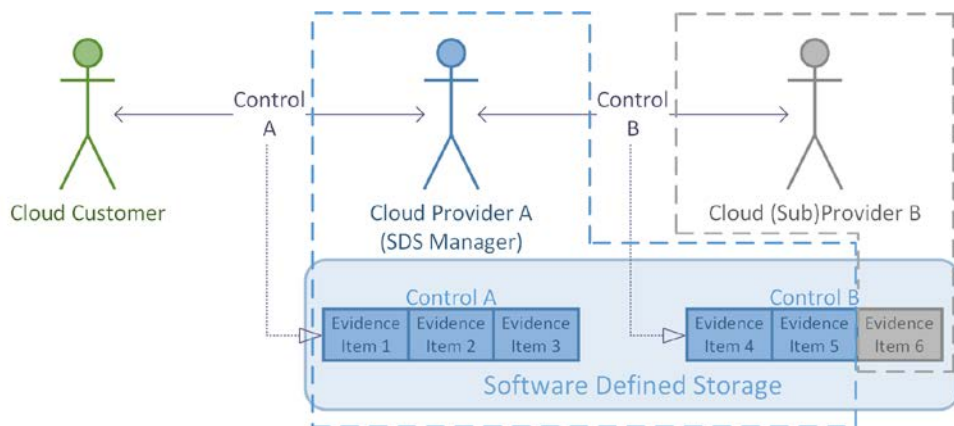


Figure 70: Desirable requirements for access control

Three of the major software defined storage platforms – OpenStack Swift, Google Cloud Storage, and Amazon S3 – have a two-level hierarchy where the upper level serves as a container for the objects which contain the relevant information to be stored (note that “Containers” are called in OpenStack Swift and Google Cloud Storage whereas “buckets” are called in Amazon S3). One can think of a container as a folder where only files (objects) can be stored, not allowing nested folders. The finest granularity that some software defined storage platforms (e.g. OpenStack Swift [14]) allow is per container. This means that a user who is granted access rights to a specific container (Control) may then access all its objects (Evidence Items) – depicted in Figure 71. In order to support object-level access control, additional security mechanisms that allow finer access granularity are required.

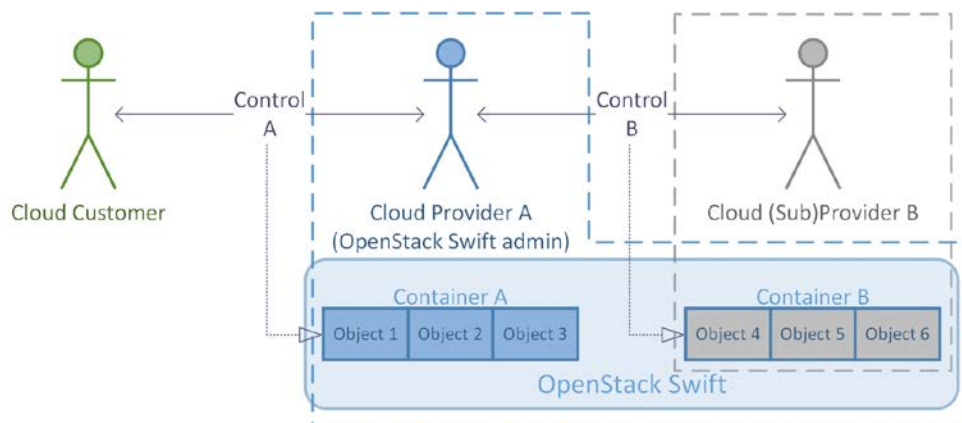


Figure 71: Access control using OpenStack Swift.

Alongside access control, there are other security and privacy concerns that need to be addressed. As an example, integrity checks must be enforced in order to guarantee that the Evidence Items kept in the software defined storage platform have not been tampered with. Enabling monitoring of events at the object level could be useful in small scenarios. However, this may involve dealing with a remarkable amount of data in large scenarios, making it a hardly scalable solution. In scenarios where two different cloud providers need to share the same Evidence Items, there is a risk of data aggregation. If this situation is likely to arise, additional mechanisms which filter the shared information to specific actors should be implemented – for example, transparency logs [15].

6.4 Assurance for the Demonstrator Scenario

The main goal for accountability is to increase trust in cloud computing by devising methods and tools, through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in the cloud. The Cloud Accountability Project (A4Cloud) has specified an accountability model for cloud supply chains [4] and several tools to support accountability have been implemented. In order to prove the application of the accountability model and related tools, a demonstrator scenario has been developed. In this section, the demonstrator scenario is taken into account in order to provide assurance, hence the provision of the account. Wearable Co. is a manufacturer of wearable devices

that collect well-being data from its wearers. It uses the SaaS (Software as a Service) provider Kardio-Mon to provide additional services to its customers. Kardio-Mon integrates Map-on-Web's services into their own. Kardio-Mon and Map-on-Web use the IaaS (Infrastructure as a Service) provider DataSpacer to run their services. This scenario is depicted in Figure 72, where the interactions among the different actors have been numbered. For the sake of simplicity, only interactions between two actors have been considered.

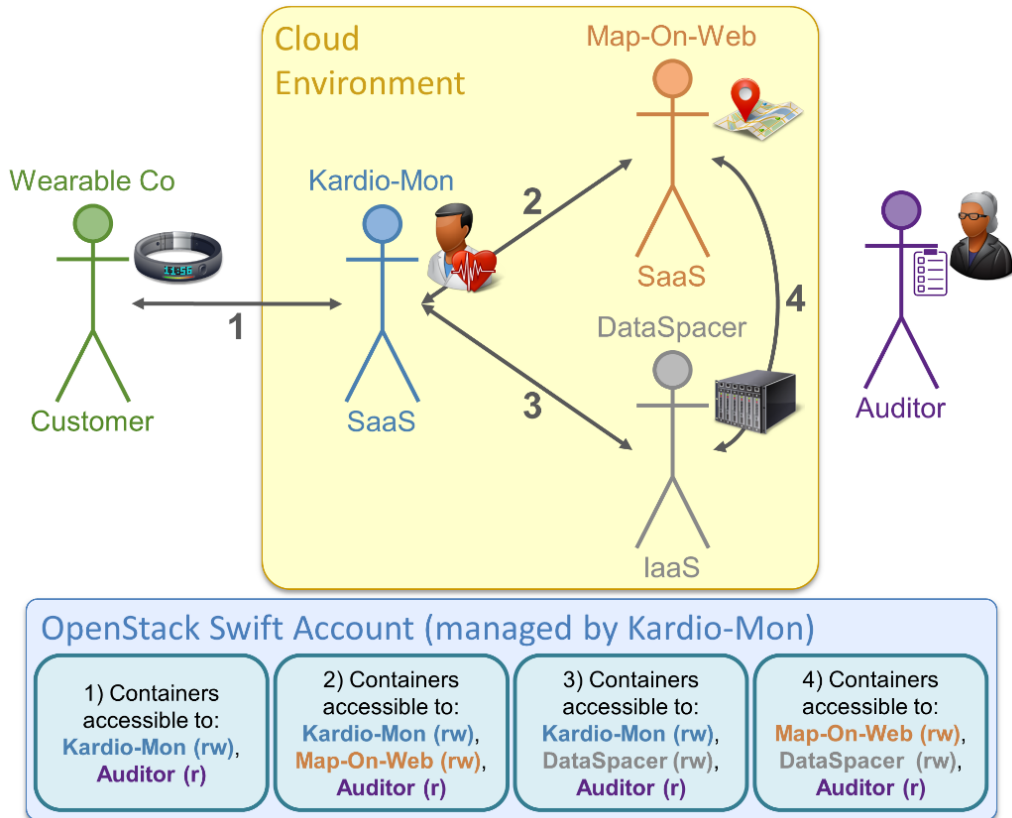


Figure 72: Wearable service demonstrator scenario: environment and storage platform with access permissions.

These interactions are subject to be monitored (implementing controls), either continuously or occasionally. The evidence collected to support this process, supplied by the different cloud providers, will be stored in an OpenStack Swift server whose administrator will be Kardio-Mon. The reasons to use this platform are that the demonstrator scenario for the Cloud Accountability Project uses an OpenStack deployment and also because it is open-source. In the event of having an external auditor to audit these controls, she will require access to read this evidence. Figure 72 shows also the access permissions for all actors involved in the demonstrator use case (Note that each control will be associated with a container in OpenStack Swift).

6.4.1 An Assurance Example: Implementing SLAs

Given the scenario presented in the previous section, let's consider an example where service level agreements (SLA) among the different cloud providers are to be implemented and reviewed, as defined in control STA-07 from the CSA Cloud Control Matrix (see Table 4). Each SLA will be considered as a separate Control. For the sake of simplicity we will ignore one of the cloud providers (Map-On-Web) and we will focus on two SLAs: 1) Wearable Co and Kardio-Mon, and 2) Kardio-Mon and DataSpacer. The case of having an external auditor in the system will also be considered. As specified previously, Kardio-Mon will be the OpenStack Swift server administrator. Each Control – one per SLA – needs to be associated with a container in OpenStack Swift. These will be named STA-07-SLA1 and STA-07-SLA2. Kardio-Mon is responsible for creating them and for granting the expected access rights. Let's consider that each Control requires only three types of evidence to support its proper operation: 1) the SLA definition, 2) some performance metrics, and 3) some operation logs. Let us consider that Kardio-Mon is the cloud provider in charge of supplying the SLA definitions and the updated performance metrics.

The logs are to be supplied by the cloud provider running the service. This means that Kardio-Mon is responsible for all the Evidence Items from Control STA-07-SLA1 and for the SLA definition and performance metrics for STA-07-SLA2. With respect to DataSpacer, it should only provide the logs for STA-07-SLA2. This scenario is depicted in Figure 73.

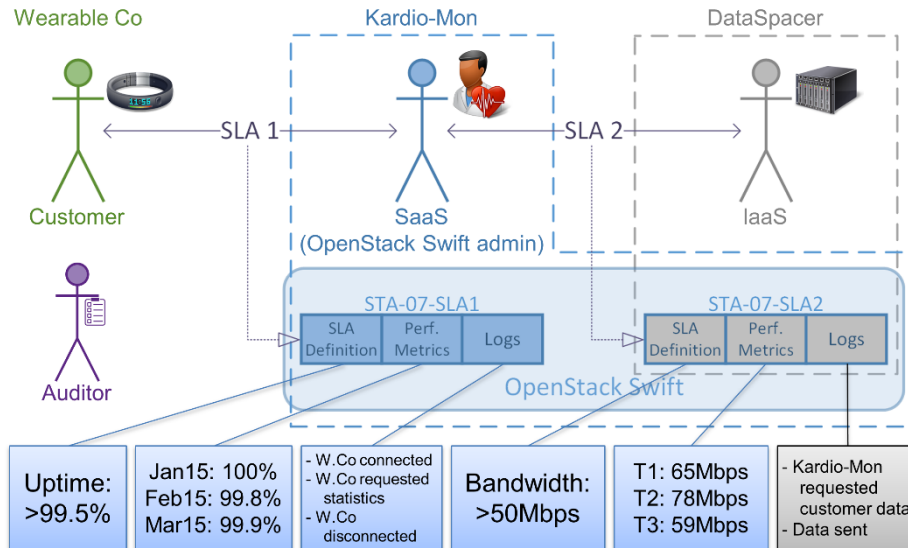


Figure 73: Example of a cloud environment with SLAs in place.

6.4.2 Demonstrator Access Configuration

It is necessary to configure the evidence collection in such a way that both Kardio-Mon and DataSpacer are able to access the evidence from Control STA-07-SLA2. Consequently, it needs to be ensured that none of the cloud providers have modified – either intentionally or accidentally – the evidence whose responsibility falls on the other provider. As an auditor is to be expected to join the scenario, her access rights should be set in OpenStack Swift. She should be granted reading permissions to all the Controls. On a different note, the role of Wearable Co is limited to cloud customer, hence not being part of the cloud. Therefore, it should have no access rights whatsoever to the storage platform. All the access rights are collected in Figure 74.

Actor	Wearable Co		Kardio-Mon		DataSpacer		Auditor	
Operation	Read	Write	Read	Write	Read	Write	Read	Write
SDS*	✗	✗	✓	✓	✗	✗	✗	✗
SLA1	✗	✗	✓	✓	✗	✗	✓	✗
SLA2	✗	✗	✓	✓	✓	✓	✓	✗

*SDS: Create/Delete containers and modify privileges

Figure 74: Access rights for the different actors.

Wearable Co is the one who, ultimately, is interested in receiving assurance that the data that it puts in the cloud will be adequately protected using privacy and security measures. This assurance may be provided by an external auditor or by an auditor within the cloud environment. In the latter case, one of the cloud providers should act as an auditor, providing comprehensive assurance about the cloud supply chain to the customer. Note that this system can be used as well for such internal auditing.

6.5 Security and Privacy Assurance Case Environment

This section has briefly discussed security and privacy assurance in cloud ecosystems and provided some guidelines on how it can be implemented throughout a cloud supply chain. The controls to be set

should be associated with evidence that supports compliance with security and privacy policies. This evidence should be saved in a permanent storage platform accessible to the different cloud providers. The discussion provides a rationale for the assurance problem in the cloud and highlights some preliminary requirements. In order to provide support for security and privacy assurance throughout the cloud supply chain, it is necessary:

- to regard security and privacy solutions as deployed across the cloud supply chain rather than from a single organisation viewpoint,
- to design and implement means for supporting assurance,
- to understand emergent dependencies among security and privacy solutions deployed in cloud ecosystems,
- to assess how security and privacy solutions comply with (or enable to comply with) organisational as well as regulatory policies,
- to gather operational evidence that supports security and privacy assurance across the cloud supply chain.

At the Hewlett Packard Labs, within the Cloud Accountability Project (A4Cloud), we have implemented a system called Security and Privacy Assurance Case Environment (SPACE), which helps gathering and classifying assurance evidence and controls (configured according to the user access rights for the demonstrator scenario). Figure 75 is a SPACE screenshot, which shows a list of claims, arguments, controls and evidence that are mapped to the demonstrator scenario and that can be monitored in order to provide assurance.

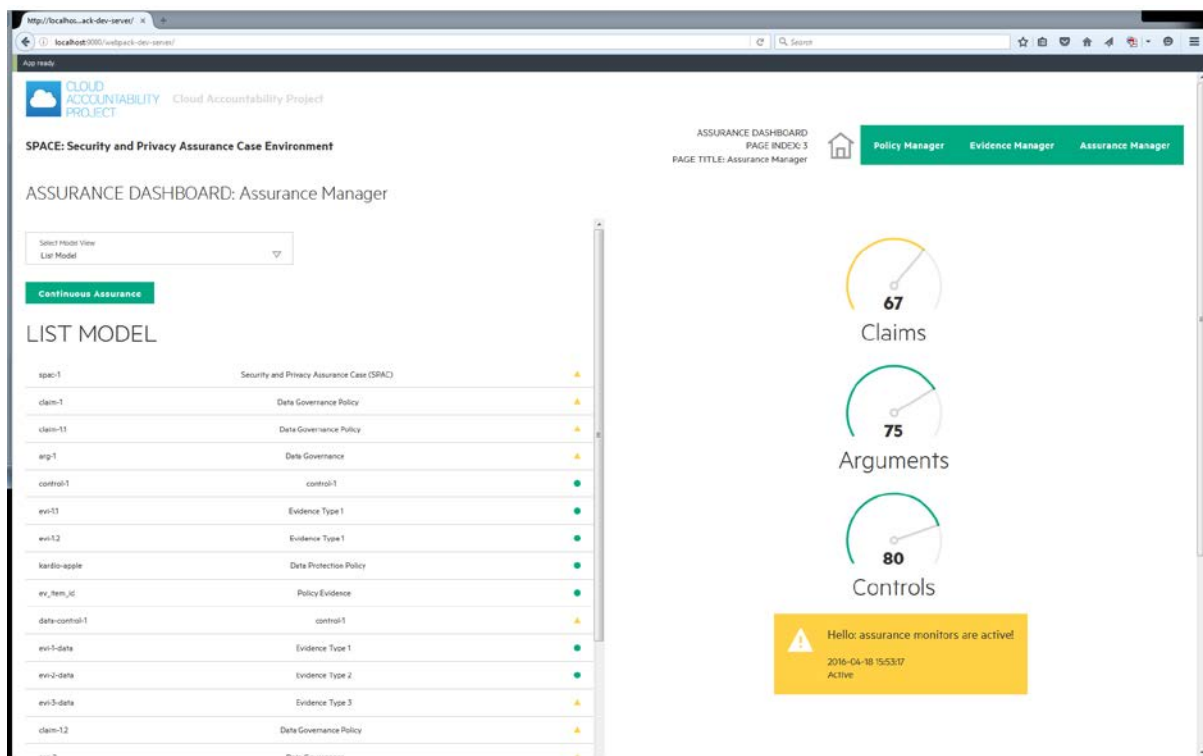


Figure 75: Security and Privacy Assurance Case Environment (SPACE).

The operational evidence supporting the controls, hence the arguments and claims can be monitored and quantified in order to provide an account of how compliance to high level policies (associated to claims) is achieved operationally. For example, the screenshot shows the case on a partial compliance due to some evidence not supporting (or failing some auditing tasks). Therefore, SPACE can be used to monitor how security and privacy controls as well as accountability mechanisms (such as the ones implemented by the Cloud Accountability Project) support policy compliance in operational environments, hence it provides an account of how organisation is accountable. SPACE eases auditing

the cloud supply chain, eventually contributing to providing security and privacy assurance, hence supporting the provision of the account.

7 Conclusions

This deliverable comprises the final version of the A4Cloud use case instantiation describing the application of the Cloud Accountability Reference Architecture for the implementation of a real life scenario in the wearables sector. More specifically, the document presented how the reference architecture is instantiated for the wearables use case and how the A4Cloud tools can integrate with the use case implementation to support the identified business actors in such a cloud environment to be accountable when delivering a cloud service, which collects and processes personal data from wearable devices.

The work performed in the context of this deliverable has resulted in the delivery of the wearables use case, which demonstrates the implementation of the accountability reference architecture and the use of the respective A4Cloud tools in a real life example of a cloud service chain, which exhibits certain security and privacy concerns. This use case serves the privacy and data protection requirements of the wearables domain and showcases how the involved business actors should adopt accountability mechanisms to ensure that the collection and processing of customers' personal data from wearable devices are handled responsibly, based on the established regulations and the declared organisational policies, which address specific security and privacy requirements.

Through the final instantiation of the A4Cloud use case prototype, we present an integrated end to end approach for the support of accountability along the cloud service supply chain comprising the wearable cloud service. Thus, this deliverable presented how the results of the A4Cloud project work for each of the relevant cloud actors, embodying a particular cloud and data protection role in the provision of the wearables use case. Through this final prototype, we managed to demonstrate the adoption of the accountability support services and artefacts across the various phases of the lifecycle for accountability giving the perspective of the involved business actors and illustrating how the A4Cloud tools are integrated and interoperate to implement the accountability mechanisms for each of them in the cloud service supply chain.

To this end, the deliverable succeeds in presenting an accountability based analysis of the wearables use case and providing the implementation of an integrated proof of concept demonstrator for the A4Cloud prototype. This use case prototype includes the integration of the A4Cloud tools and their customisation into the wearables use case, while it demonstrates the support for accountability from the perspective of the different roles, namely the cloud provider, the cloud customer, the data subject and the cloud auditor. Through the five demonstration scenarios presented in Section 5, we have managed to address the view of all these roles in the implementation of accountability. Further to it, we have compiled a guidance section to help the developers of use case applications in the cloud to understand how to instantiate the cloud accountability reference architecture and integrate the respective A4Cloud tools for the implementation of accountability mechanisms in their application.

Moving from the theory to practice, the work in this deliverable allowed us to learn that the implementation of accountability across a complex cloud service environment is not an easy task. Both the implementation of the necessary mechanisms and the demonstration of the actors' compliance with the regulations and the policies needs a continuous effort for providing an account. The tools required to support the implementation of accountability can provide a level of automation for the execution of the relevant practices, but, by no means, can they substitute the involvement of the human factor is assessing the compliance of the cloud environment with the data protection requirements. However, the end to end approach that was presented in this deliverable reflects the capabilities of the technology to support cloud providers and customers in accepting the responsibilities attributed to them through the regulations and adopting an evidence based attitude to provide an assurance on their collection and processing procedures of personal data involved in their cloud business.

8 References

- [1] A4Cloud, Deliverable D32.1: "D:C-2.1 Report detailing conceptual framework", October 2014.
- [2] A4Cloud, Deliverable D47.1: " D:D-7.1: First system and use case prototype", May 2015.
- [3] A4Cloud, Deliverable D42.4a: " D:D-2.4a: Cloud Accountability Reference Architecture", March 2016.
- [4] Felici, M., Pearson, S.: Accountability for Data Governance in the Cloud. In Felici, M., Fernández-Gago, C (Eds.), Accountability and Security in the Cloud, A4Cloud 2014, Springer, LNCS 8937, pp. 3-42, 2015.
- [5] Felici, M.: Cloud Accountability: Glossary of Terms and Definitions. In Felici, M., Fernán-dez-Gago, C (Eds.), Accountability and Security in the Cloud, A4Cloud 2014, Springer, LNCS 8937, pp. 291-306, 2015.
- [6] ENISA: Privacy, Accountability and Trust – Challenges and Opportunities. European Network and Information Security Agency (ENISA), 2011.
- [7] Baldwin, A., Pym, D., Shiu, S.: Enterprise Information Risk Management: Dealing with Cloud Computing. In S. Pearson, S., Yee, G. (Eds.), Privacy and Security for Cloud Computing, Springer-Verlag, 2013.
- [8] CSA: The Notorious Nine Cloud Computing Top Threats in 2013. Top Threats Working Group, Cloud Security Alliance, 2013.
- [9] Pearson, S.: Accountability in Cloud Service Provision Ecosystems, Springer, 2014.
- [10] Cloud Security Alliance (CSA): Cloud Control Matrix v3.0.1, October 2014.
- [11] National Institute of Standards and Technology (NIST): NIST Cloud Computing Security Reference Architecture, Special Publication 500-299.
- [12] Computer Sciences Corporation (CSC): A Precipice for the CloudTrust Protocol (V2.0), 2010.
- [13] Włodarczyk, T. W., Pais, R. (Eds.): Framework of evidence (final), A4Cloud Deliverable D38.2, 2015.
- [14] Arnold, J.: OpenStack Swift, O'Reilly, 2015.
- [15] Pulls. T.: Preserving Privacy in Transparency Logging. Doctoral dissertation, Karlstads Universitet, 2015.

9 Appendices

9.1 Specifications of the wearable use case

9.1.1 The list of personal data

In the wearables use case, we define the following list of personal data, as shown in Table 5.

Table 5: Type of data comprising the profile of the Wearable Co customers

Data Name	Data Description	Type of personal data
Username	The username used as user credentials, along with the password, to log in to the Wearable Service	Sensitive
Password	The password used as user credentials, along with the username, to log in to the Wearable Service	Sensitive
User ID	The unique identification number assigned to the user in order to accomplish user specific actions within a session life time	Sensitive
Display Name	The nickname selected by the user to display on the Wearable Service front end, as a comprehensive user reference	Public
Gender	The gender of the user to be used for determining the threshold values applied to the collected wellbeing metric values. Gender is considered to affect the optimal values determining the threshold values.	Public
Age	The age of the user to be used for determining the threshold values applied to the collected wellbeing metric values. Different age groups are considered to have different optimal values determining the threshold values.	Public
Height	The height of the user to be used for determining wellbeing related information by joining up the wellbeing record with the body type.	Sensitive
Weight	The weight of the user to be used for determining wellbeing related information by joining up the wellbeing record with the body type.	Sensitive
Sugar Level	The sugar level in the user's blood, measured by the wearable device	Sensitive
Blood Pressure	The user's blood pressure, measured by the wearable device	Sensitive
Heartbeat Rate	The user's heart beat rate, measured by the wearable device	Sensitive
Training Activity	The daily exercises taken by the user, such as time of walking, running, swimming and any other physical exercise	Sensitive
Country	The country of permanent residence of the user	Public

9.1.2 The machine readable accountability policy

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE a-ppl:Policy>
<a-ppl:Policy
  xmlns:ob="http://www.a4cloud.eu/a-ppl/obligation"
  ppl="http://www.a4cloud.eu/a-ppl"
  xmlns:a-
```

```
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyId="WearableCo-Policy"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides">

  <!-- The personal data that will be stored are defined here -->

  <xacml:Target>
    <xacml:Resources>
      <xacml:Resource>
        <xacml:ResourceMatch
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml:AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">username</xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator
              DataType="http://www.w3.org/2001/XMLSchema#string"
              AttributeId="resource:resource-type" />
            </xacml:ResourceMatch>
          </xacml:Resource>
          <xacml:Resource>
            <xacml:ResourceMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <xacml:AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">password</xacml:AttributeValue>
                <xacml:ResourceAttributeDesignator
                  DataType="http://www.w3.org/2001/XMLSchema#string"
                  AttributeId="resource:resource-type" />
                </xacml:ResourceMatch>
              </xacml:Resource>
              <xacml:Resource>
                <xacml:ResourceMatch
                  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <xacml:AttributeValue
                      DataType="http://www.w3.org/2001/XMLSchema#string">user id</xacml:AttributeValue>
                    <xacml:ResourceAttributeDesignator
                      DataType="http://www.w3.org/2001/XMLSchema#string"
                      AttributeId="resource:resource-type" />
                    </xacml:ResourceMatch>
                  </xacml:Resource>
                  <xacml:Resource>
                    <xacml:ResourceMatch
                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
                          DataType="http://www.w3.org/2001/XMLSchema#string">display
name</xacml:AttributeValue>
                        <xacml:ResourceAttributeDesignator
                          DataType="http://www.w3.org/2001/XMLSchema#string"
                          AttributeId="resource:resource-type" />
                        </xacml:ResourceMatch>
                      </xacml:Resource>
                      <xacml:Resource>
                        <xacml:ResourceMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <xacml:AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#string">gender</xacml:AttributeValue>
                            <xacml:ResourceAttributeDesignator
                              DataType="http://www.w3.org/2001/XMLSchema#string"
                              AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                          </xacml:Resource>
                          <xacml:Resource>
                            <xacml:ResourceMatch
                              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```

        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">date
birth</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">country</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">email</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">height</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">weight</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">sugar
level</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

```



```

        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">blood
pressure</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">heartbeat
rate</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">workout</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">yoga</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">swimming</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>
<xacml:Resource>
    <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">running</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type"
        ResourceSchema="https://schema.org/MedicalCondition" />
    </xacml:ResourceMatch>
</xacml:Resource>

```

```
        </xacml:Resources>
    </xacml:Target>

    <!-- Rule for personal data accessing by Data Subjects (Clients of WearableCo)-->
    <!-- Rule1: All PII can be read, updated or deleted by Data Subject-->
    <a-ppl:Rule Effect="Permit" RuleId="a-ppl_rule_1">
        <xacml:Target>
            <xacml:Subjects>
                <xacml:Subject>
                    <xacml:SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Data
Subject</xacml:AttributeValue>
                        <xacml:SubjectAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="subject:subject-id"/>
                    </xacml:SubjectMatch>
                </xacml:Subject>
            </xacml:Subjects>
            <xacml:Actions>
                <xacml:Action>
                    <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</xacml:AttributeValue>
                        <xacml:ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                    </xacml:ActionMatch>
                </xacml:Action>
                <xacml:Action>
                    <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">update</xacml:AttributeValue>
                        <xacml:ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                    </xacml:ActionMatch>
                </xacml:Action>
                <xacml:Action>
                    <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</xacml:AttributeValue>
                        <xacml:ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                    </xacml:ActionMatch>
                </xacml:Action>
            </xacml:Actions>
        </xacml:Target>
    </a-ppl:Rule>

    <!-- WearableCo's access control policy -->
    <!-- Rule 2: referring to access to personal data for WearableCo Employees -->
    <a-ppl:Rule Effect="Permit" RuleId="a-ppl_rule_2">
        <xacml:Target>
            <xacml:Subjects>
                <xacml:Subject>
                    <xacml:SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Employee</xacml:AttributeValue>
```

```

        <xacml:SubjectAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="subject:subject-id"/>
      </xacml:SubjectMatch>
    </xacml:Subject>
  </xacml:Subjects>
  <xacml:Resources>
    <xacml:Resource>
      <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">username</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
      </xacml:Resource>
    <xacml:Resource>
      <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">display
          name</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
      </xacml:Resource>
    <xacml:Resource>
      <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">gender</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
      </xacml:Resource>
    <xacml:Resource>
      <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">date
          birth</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
      </xacml:Resource>
    <xacml:Resource>
      <xacml:ResourceMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">country</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
          DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
      </xacml:Resource>
    <xacml:Resource>
      <xacml:ResourceMatch

```

```

        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">email</xacml:AttributeValue>
        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
        </xacml:ResourceMatch>
        </xacml:Resource>
    </xacml:Resources>
    <xacml:Actions>
        <xacml:Action>
            <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</xacml:AttributeValue>
                <xacml:ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                </xacml:ActionMatch>
            </xacml:Action>
        </xacml:Actions>
    </xacml:Target>
</a-ppl:Rule>

<!-- WearableCo's access control policy for Map-On-Web -->
<!-- Rule 3: NON downstream usage -->
<a-ppl:Rule Effect="Permit" RuleId="a-ppl_rule_3">
    <xacml:Target>
        <xacml:Subjects>
            <xacml:Subject>
                <xacml:SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Map-On-
Web</xacml:AttributeValue>
                    <xacml:SubjectAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="subject:subject-id"/>
                    </xacml:SubjectMatch>
                </xacml:Subject>
            </xacml:Subjects>
            <xacml:Resources>
                <xacml:Resource>
                    <xacml:ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">date
birth</xacml:AttributeValue>
                        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
                        </xacml:ResourceMatch>
                    </xacml:Resource>
                <xacml:Resource>
                    <xacml:ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">blood
pressure</xacml:AttributeValue>
                        <xacml:ResourceAttributeDesignator
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
                        </xacml:ResourceMatch>
                    </xacml:Resource>

```

of

```

        <xacml:Resource>
          <xacml:ResourceMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
            <xacml:AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">sugar
              level</xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator
              DataType="http://www.w3.org/2001/XMLSchema#string"
              AttributeId="resource:resource-type" />
            </xacml:ResourceMatch>
          </xacml:Resource>
        <xacml:Resource>
          <xacml:ResourceMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
            <xacml:AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">heartbeat
              rate</xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator
              DataType="http://www.w3.org/2001/XMLSchema#string"
              AttributeId="resource:resource-type" />
            </xacml:ResourceMatch>
          </xacml:Resource>
        <xacml:Resource>
          <xacml:ResourceMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
            <xacml:AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">country</xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator
              DataType="http://www.w3.org/2001/XMLSchema#string"
              AttributeId="resource:resource-type" />
            </xacml:ResourceMatch>
          </xacml:Resource>
        </xacml:Resources>
      <xacml:Actions>
        <xacml:Action>
          <xacml:ActionMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml:AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">read</xacml:AttributeValue>
            <xacml:ActionAttributeDesignator
              DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
            </xacml:ActionMatch>
          </xacml:Action>
        </xacml:Actions>
      </xacml:Target>
    </a-ppl:Rule>

    <!-- WearableCo's data handling policy -->
    <a-ppl:DataHandlingPolicy>
      <a-ppl:AuthorizationsSet>

        <!-- Personal Data should be used from Wearable Co only for the following
purposes -->

        <a-ppl:AuthzUseForPurpose>
          <a-ppl:Purpose
            location="Europe">http://www.w3.org/2002/01/P3Pv1/health</a-ppl:Purpose>
            duration="P2Y6M0DT00H0M0S"
          <a-ppl:Purpose
            location="Europe">http://www.w3.org/2002/01/P3Pv1/admin</a-ppl:Purpose>
            duration="P2Y6M2DT00H0M0S"
          </a-ppl:AuthzUseForPurpose>

        <!-- Policy for third party data processors (Map-On-Web data provider) -
->

```

```

    <!-- This policy has more "strict" rules -->
    <a-ppl:AuthzDownstreamUsage allowed="false">
        <a-ppl:Policy xmlns:ob="http://www.a4cloud.eu/a-ppl/obligation"
            xmlns:a-ppl="http://www.a4cloud.eu/a-
ppl" xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" PolicyId="MapOnWeb-Policy"

RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides">

            <xacml:Target>
                <xacml:Resources>
                    <xacml:Resource>
                        <xacml:ResourceMatch

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Age</xacml:AttributeValue>
                            <xacml:ResourceAttributeDesignator

DataType="http://www.w3.org/2001/XMLSchema#string"
                                AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                        </xacml:Resource>
                    <xacml:Resource>
                        <xacml:ResourceMatch

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Blood
Pressure</xacml:AttributeValue>
                            <xacml:ResourceAttributeDesignator

DataType="http://www.w3.org/2001/XMLSchema#string"
                                AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                        </xacml:Resource>
                    <xacml:Resource>
                        <xacml:ResourceMatch

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Sugar
Level</xacml:AttributeValue>
                            <xacml:ResourceAttributeDesignator

DataType="http://www.w3.org/2001/XMLSchema#string"
                                AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                        </xacml:Resource>
                    <xacml:Resource>
                        <xacml:ResourceMatch

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Heartbeat
Rate</xacml:AttributeValue>
                            <xacml:ResourceAttributeDesignator

DataType="http://www.w3.org/2001/XMLSchema#string"
                                AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                        </xacml:Resource>
                    <xacml:Resource>
                        <xacml:ResourceMatch

```



```
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Country</xacml:AttributeValue>
    <xacml:ResourceAttributeDesignator

DataType="http://www.w3.org/2001/XMLSchema#string"
        AttributeId="resource:resource-type" />
    </xacml:ResourceMatch>
</xacml:Resource>
</xacml:Resources>
</xacml:Target>

<!-- Rule for personal data accessing by Map-On-Web provider -->
<!-- All data can be read or deleted by Map-On-Web from it's
database -->
    <a-ppl:Rule Effect="Permit" RuleId="a-ppl_rule_1">
        <xacml:Target>
            <xacml:Subjects>
                <xacml:Subject>
                    <xacml:SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Map-On-
Web</xacml:AttributeValue>
                        <xacml:SubjectAttributeDesignator
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            AttributeId="subject:subject-id"/>
                        </xacml:SubjectMatch>
                    </xacml:Subject>
                </xacml:Subjects>
                <xacml:Actions>
                    <xacml:Action>
                        <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</xacml:AttributeValue>
                                <xacml:ActionAttributeDesignator
                                    DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                                </xacml:ActionMatch>
                            </xacml:Action>
                        <!-- Point out that access to delete must be agreed
to Map-On-Web to ATC -->
                            <xacml:Action>
                                <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                    <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</xacml:AttributeValue>
                                    <xacml:ActionAttributeDesignator
                                        DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="action:action-id"/>
                                    </xacml:ActionMatch>
                                </xacml:Action>
                            </xacml:Actions>
                        </xacml:Target>
                    </a-ppl:Rule>

                    <!-- Map-On-Web's data handling policy -->
                    <a-ppl:DataHandlingPolicy>
                        <a-ppl:AuthorizationsSet>

                            <!-- Personal Data should be used from Map-On-Web only
for the following purposes -->
                            <a-ppl:AuthzUseForPurpose>
                                <a-ppl:Purpose
                                    location="Europe">http://www.w3.org/2002/01/P3Pv1/health</a-ppl:Purpose>
                                </a-ppl:AuthzUseForPurpose>
```

```
<!-- Map-On-Web is not allowed to send Personal Data to
third party data processors -->
<a-ppl:AuthzDownstreamUsage allowed="false"/>
</a-ppl:AuthorizationsSet>

<!-- Wearable Co is accountable to their customers for how
data are processed by Map-On-Web-->
<ob:ObligationsSet>
  <ob:Obligation elementId="a-ppl_rule_2">
    <ob:TriggersSet>
      <ob:TriggerPersonalDataAccessedForPurpose>
        <a-
ppl:Purpose>http://www.w3.org/2002/01/P3Pv1/health</a-ppl:Purpose>
      </ob:TriggerPersonalDataAccessedForPurpose>
    </ob:TriggersSet>
    <ob:ActionLog>
      <ob:Timestamp>true</ob:Timestamp>
      <ob:Action>true</ob:Action>
      <ob:Purpose>true</ob:Purpose>
      <ob:Subject>true</ob:Subject>
      <ob:Resource>true</ob:Resource>
      <ob:Location>false</ob:Location>
      <ob:Expiration>false</ob:Expiration>
      <ob:Flag>false</ob:Flag>
    </ob:ActionLog>
  </ob:Obligation>

  <!--Personal Data storage period of 6 months -->
  <ob:Obligation elementId="a-ppl_rule_3">
    <ob:TriggersSet>
      <ob:TriggerAtTime>
        <ob:Start>
          <ob:StartNow />
        </ob:Start>
      <ob:MaxDelay>

<ob:Duration>P0Y0M0DT0H2M0S</ob:Duration>
      </ob:MaxDelay>
    </ob:TriggerAtTime>
  </ob:TriggersSet>
  <ob:ActionDeletePersonalData/>
</ob:Obligation>

<!-- Notification of Cardio Mon about security breach
(data loss) -->
<ob:Obligation elementId="a-ppl_rule_4">
  <ob:TriggersSet>
    <ob:TriggerDataLost/>
  </ob:TriggersSet>
  <ob:ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>cardio.mon@a4cloud.com</ob:Address>
    <ob:Recipients>Cardio Mon</ob:Recipients>
    <ob:Type>Data Lost</ob:Type>
  </ob:ActionNotify>
</ob:Obligation>

<!--Notification of Cardio Mon about security breach
(policy violation) -->
<ob:Obligation elementId="a-ppl_rule_5">
  <ob:TriggersSet>
    <ob:TriggerOnViolation/>
  </ob:TriggersSet>
  <ob:ActionNotify>
    <ob:Media>e-mail</ob:Media>
```

```

        <ob:Address>cardio.mon@a4cloud.com</ob:Address>
        <ob:Recipients>Cardio Mon</ob:Recipients>
        <ob:Type>Policy violation</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>

<!-- Other security and privacy measures -->

<!-- Log whenever access is permitted-->
<ob:Obligation elementId="a-ppl_rule_6">
    <ob:TriggersSet>
        <!-- A-PPL trigger -->
        <ob:TriggerPersonalDataAccessPermitted/>
    </ob:TriggersSet>
    <!-- A-PPL log action -->
    <ob:ActionLog>
        <ob:Timestamp>true</ob:Timestamp>
        <ob:Action>true</ob:Action>
        <ob:Purpose>true</ob:Purpose>
        <ob:Subject>true</ob:Subject>
        <ob:Resource>true</ob:Resource>
        <ob:Location>false</ob:Location>
        <ob:Expiration>false</ob:Expiration>
        <ob:Flag>false</ob:Flag>
    </ob:ActionLog>
</ob:Obligation>

<!-- Notify Cardio Mon whenever access is denied-->
<ob:Obligation elementId="a-ppl_rule_7">
    <ob:TriggersSet>
        <ob:TriggerPersonalDataAccessDenied/>
    </ob:TriggersSet>
    <ob:ActionNotify>
        <ob:Media>e-mail</ob:Media>
        <ob:Address>cardio.mon@a4cloud.com</ob:Address>
        <ob:Recipients>Cardio Mon</ob:Recipients>
        <ob:Type>Unauthorized Personal Data Access
Attempt</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>

<!-- Notify Cardio Mon whenever personal data are
deleted-->

<ob:Obligation elementId="a-ppl_rule_8">
    <ob:TriggersSet>
        <ob:TriggerPersonalDataDeleted/>
    </ob:TriggersSet>
    <ob:ActionNotify>
        <ob:Media>e-mail</ob:Media>
        <ob:Address>cardio.mon@a4cloud.com</ob:Address>
        <ob:Recipients>Cardio Mon</ob:Recipients>
        <ob:Type>Personal Data Deleted</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>
</ob:ObligationsSet>
</a-ppl:DataHandlingPolicy>
</a-ppl:Policy>
</a-ppl:AuthzDownstreamUsage>
</a-ppl:AuthorizationsSet>

<!-- Wearable Co obligations (accountable to their customers) -->
<ob:ObligationsSet>
    <!--Notification of data subject when she is registered to the application
for the first time. Data then is about to be collected -->
    <!-- Information about collecting and processing, purpose, location,
recipients,

```

```
rights -->
<ob:Obligation elementId="a-ppl_rule_2">
  <ob:TriggersSet>
    <ob:TriggerOnUserRegistration />
  </ob:TriggersSet>
  <!-- A-PPL action -->
  <ob:ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>data.subject@a4cloud.com</ob:Address>
    <ob:Recipients>Data Subject</ob:Recipients>
    <ob:Type>Data Collection</ob:Type>
  </ob:ActionNotify>
</ob:Obligation>

<!-- Notification of Data Protection Authority (DPA) that data is about
to be collected -->
<ob:Obligation elementId="a-ppl_rule_3">
  <ob:TriggersSet>
    <ob:TriggerOnDataCollection />
  </ob:TriggersSet>
  <!-- A-PPL action -->
  <ob:ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>dpa@a4cloud.com</ob:Address>
    <ob:Recipients>Data Protection Authority</ob:Recipients>
    <ob:Type>Data Collection</ob:Type>
  </ob:ActionNotify>
</ob:Obligation>

<!-- Wearable Co is accountable for collecting, processing data only for
specific purposes -->
<ob:Obligation elementId="a-ppl_rule_4">
  <ob:TriggersSet>
    <ob:TriggerPersonalDataAccessedForPurpose>
      <a-ppl:Purpose duration="P1Y0M0DT00H02M0S"
location="Europe">http://www.w3.org/2002/01/P3Pv1/health</a-ppl:Purpose>
      <a-ppl:Purpose duration="P1Y0M0DT00H02M0S"
location="Europe">http://www.w3.org/2002/01/P3Pv1/admin</a-ppl:Purpose>
    </ob:TriggerPersonalDataAccessedForPurpose>
  </ob:TriggersSet>
  <ob:ActionLog>
    <ob:Timestamp>true</ob:Timestamp>
    <ob:Action>true</ob:Action>
    <ob:Purpose>true</ob:Purpose>
    <ob:Subject>true</ob:Subject>
    <ob:Resource>true</ob:Resource>
    <ob:Location>false</ob:Location>
    <ob:Expiration>false</ob:Expiration>
    <ob:Flag>false</ob:Flag>
  </ob:ActionLog>
</ob:Obligation>

<!--Personal Data storage period of 1 year -->
<ob:Obligation elementId="a-ppl_rule_5">
  <ob:TriggersSet>
    <ob:TriggerAtTime>
      <ob:Start>
        <ob:StartNow />
      </ob:Start>
      <ob:MaxDelay>
        <ob:Duration>P0Y1M0DT0H1M0S</ob:Duration>
      </ob:MaxDelay>
    </ob:TriggerAtTime>
  </ob:TriggersSet>
  <ob:ActionDeletePersonalData />
```

```
</ob:Obligation>

<!-- Ask Data Subject for consent to processing -->
<ob:Obligation elementId="a-ppl_rule_6">
  <ob:TriggersSet>
    <ob:TriggerOnUserRegistration />
  </ob:TriggersSet>
  <ob>ActionRequestConsent />
</ob:Obligation>

<!-- Notification of DS about security breach (data loss) -->
<ob:Obligation elementId="a-ppl_rule_7">
  <ob:TriggersSet>
    <ob:TriggerDataLost/>
  </ob:TriggersSet>
  <ob>ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>data.subject@a4cloud.com</ob:Address>
    <ob:Recipients>Data Subject</ob:Recipients>
    <ob>Type>Data Lost</ob>Type>
  </ob>ActionNotify>
</ob:Obligation>

<!--Notification of DS about security breach (policy violation) -->
<ob:Obligation elementId="a-ppl_rule_8">
  <ob:TriggersSet>
    <ob:TriggerOnViolation />
  </ob:TriggersSet>
  <ob>ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>data.subject@a4cloud.com</ob:Address>
    <ob:Recipients>Data Subject</ob:Recipients>
    <ob>Type>Policy violation</ob>Type>
  </ob>ActionNotify>
</ob:Obligation>

<!-- Other security and privacy measures -->

<!-- Log whenever access is permitted or denied -->
<ob:Obligation elementId="a-ppl_rule_9">
  <ob:TriggersSet>
    <!-- A-PPL trigger -->
    <ob:TriggerPersonalDataAccessPermitted />
    <ob:TriggerPersonalDataAccessDenied />
  </ob:TriggersSet>
  <!-- A-PPL log action -->
  <ob>ActionLog>
    <ob:Timestamp>true</ob:Timestamp>
    <ob>Action>true</ob>Action>
    <ob:Purpose>true</ob:Purpose>
    <ob:Subject>true</ob:Subject>
    <ob:Resource>true</ob:Resource>
    <ob:Location>false</ob:Location>
    <ob:Expiration>false</ob:Expiration>
    <ob:Flag>false</ob:Flag>
  </ob>ActionLog>
</ob:Obligation>

<!-- Notify DS whenever access is denied -->
<ob:Obligation elementId="a-ppl_rule_10">
  <ob:TriggersSet>
    <ob:TriggerPersonalDataAccessDenied />
  </ob:TriggersSet>
  <ob>ActionNotify>
    <ob:Media>e-mail</ob:Media>
    <ob:Address>data.subject@a4cloud.com</ob:Address>
```

```
        <ob:Recipients>Data Subject</ob:Recipients>
        <ob:Type>Unauthorized Personal Data Access Attempt</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>

<!-- Notify DS whenever personal data are deleted -->
<ob:Obligation elementId="a-ppl_rule_11">
    <ob:TriggersSet>
        <ob:TriggerPersonalDataDeleted />
    </ob:TriggersSet>
    <ob:ActionNotify>
        <ob:Media>e-mail</ob:Media>
        <ob:Address>data.subject@a4cloud.com</ob:Address>
        <ob:Recipients>Data Subject</ob:Recipients>
        <ob:Type>Personal Data Deleted</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>

<!-- Information about use of data processors -->
<ob:Obligation elementId="a-ppl_rule_12">
    <ob:TriggersSet>
        <ob:TriggerPersonalDataSent>
            <ob:Id> Personal Data of User</ob:Id>
        </ob:TriggerPersonalDataSent>
    </ob:TriggersSet>
    <!-- A-PPL action -->
    <ob:ActionNotify>
        <ob:Media>e-mail</ob:Media>
        <ob:Address>data.subject@a4cloud.com</ob:Address>
        <ob:Recipients>Data Subject</ob:Recipients>
        <ob:Type>Personal Data Sent to Data Processor</ob:Type>
    </ob:ActionNotify>
</ob:Obligation>
</ob:ObligationsSet>
</a-ppl:DataHandlingPolicy>
</a-ppl:Policy>
```

9.1.3 Machine readable policy for DTMT configuration

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ppl:Policy>
<ppl:Policy xmlns:cr="http://www.primelife.eu/ppl/credential"
    xmlns:ob="http://www.primelife.eu/ppl/obligation"
    xmlns:ppl="http://www.primelife.eu/ppl"
    xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyId="prefGroup1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
    combining-algorithm:permit-overrides">

    <!-- The Policy is given as an input to DTMT and APPLE (both located in the
    IaaS level) -->
    <!-- Data Controller is the owner of the PII (Virtual Machine ID, Volume ID,
    Image ID) -->
    <xacml:Target>
        <xacml:Subjects>
            <xacml:Subject>
                <xacml:SubjectMatch

                    MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml:AttributeValue
    DataType="http://www.w3.org/2001/XMLSchema#string">Data
    Processor</xacml:AttributeValue>
                        <xacml:SubjectAttributeDesignator
```



```
        DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="subject:subject-id" />
        </xacml:SubjectMatch>
        </xacml:Subject>
    </xacml:Subjects>
    <xacml:Resources>
        <!-- Resources are added dynamically (Virtual Machine ID, Volume
ID, Image ID) -->
        <xacml:Resource>
            <xacml:ResourceMatch

                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Virtual          Machine
ID</xacml:AttributeValue>

                        <xacml:ResourceAttributeDesignator

                            DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="resource:resource-type" />
                            </xacml:ResourceMatch>
                            </xacml:Resource>
                        </xacml:Resources>
                        <xacml:Actions>
                            <xacml:Action>
                                <xacml:ActionMatch

                                    MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">data
transfer</xacml:AttributeValue>

                                            <xacml:ActionAttributeDesignator

                                                DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="action:action-id" />
                                                </xacml:ActionMatch>
                                                </xacml:Action>
                                            </xacml:Actions>
                                            <!-- Data must be transfered only the following locations -->
                                            <xacml:Environments>
                                                <xacml:Environment

                                                    <xacml:EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                                        <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Europe</xacml:AttributeValue>
                                                            <xacml:EnvironmentAttributeDesignator

                                                                DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId=
"environment:environment-id"/>
                                                                </xacml:EnvironmentMatch>
                                                                </xacml:Environment>
                                                            </xacml:Environments>
                                                        </xacml:Target>

                                                                <!-- Rules are defined in DTMT using Drools. -->

                                                                <!-- Infrastructure Data Processor's Data Handling Policy -->
                                                                <!-- Assuming an APPLE in the IaaS level -->
                                                                <ppl:DataHandlingPolicy>
                                                                    <ob:ObligationsSet>
                                                                        <!--Notification of Data Controller upon a potential
violation detection

                                                                            from DTMT -->
                                                                        <ob:Obligation>
                                                                            <ob:TriggersSet>
```

```

        <ob:TriggerOnViolation>
        </ob:TriggerOnViolation>
    </ob:TriggersSet>
    <ob:ActionNotify>
        <ob:Media>e-mail</ob:Media>
        <ob:Address>g.giotis@atc.gr</ob:Address>
        <ob:Recipients>Data
Controller</ob:Recipients>
        <ob:Type>DTMT Policy Violation</ob:Type>
    </ob:ActionNotify>
    </ob:Obligation>
    </ob:ObligationsSet>
    </ppl:DataHandlingPolicy>
</ppl:Policy>

```

9.2 The operation of the Web-based Wearable application

The Wearable application of the Wearable Co is a Web application (see Figure 76 for the home page), which is based on the wearable service instance of Kardio-Mon and distinguishes between two application roles, namely:

- The Wearable Co customer, who enters the Web application to manage the wearable data collected from the wearable device;
- The Wearable Co employee, who uses the Web application to monitor the list of registered users and receives alerts from the runtime use of the service.



Figure 76: The home page of the Wearable service application.

9.2.1 The operations of the Wearable Co customer

The Wearable service application offers the following main pages (UI screens) for the Wearable Co customer:

- **Registration Page:** this page enables a Wearable Co customer creating a profile in the Wearable Service, by determining the credentials for logging into the service and providing profiling data to be processed by the cloud service.
- **Log-in Page:** this page enables a Wearable Co customer to be authenticated to the service.
- **Manage Profile page:** this page enables a Wearable Co customer to manage their profile data.
- **Home Page:** This page hosts the access buttons to the “request real time information” and the “get wellbeing activities” pages.
- **Request real time information page:** this page enables a Wearable Co customer to retrieve an overview of their wearable data for the blood pressure, the sugar level and the heart beat rate, normalised by the typical threshold values for each of these attributes, along with the timeline visualisation of these customer records per month.
- **Get wellbeing activities page:** this page enables a Wearable Co customer to manage their wellbeing activities per day by specifying the type and the duration of the activity (selection among yoga, running, swimming and walking activities).
- **Request map visualisation page:** This page enables a Wearable Co customer to navigate to the overall statistics of the wearable data collected from all the customers of the Wearable Service for the Wearable Co.

In the remaining part of this section we demonstrate the execution steps for this scenario of the Wearable Co customer, along with a set of screenshots visualising the pages that the Wearable Co customer goes through.

From the home page (see Figure 76), the Wearable Co customer selects the login button from the top right menu bar (highlighted by the orange dashed rectangular³). The login page is, then, displayed, as shown in Figure 77. From this page, the customer can either select to create an account (option 1) or login to the Web application, as being a registered user (option 2).

The screenshot shows a web page titled "My Account". It is divided into two main sections: "REGISTERED USER" and "CREATE AN ACCOUNT".

REGISTERED USER: This section contains two input fields, "Username" and "Password". Below the "Password" field is a blue "LOGIN" button. To the right of the "LOGIN" button is a link that says "Lost Password?". An orange ellipse highlights the "LOGIN" button and the "Lost Password?" link, with an orange square containing the number "2" next to it.

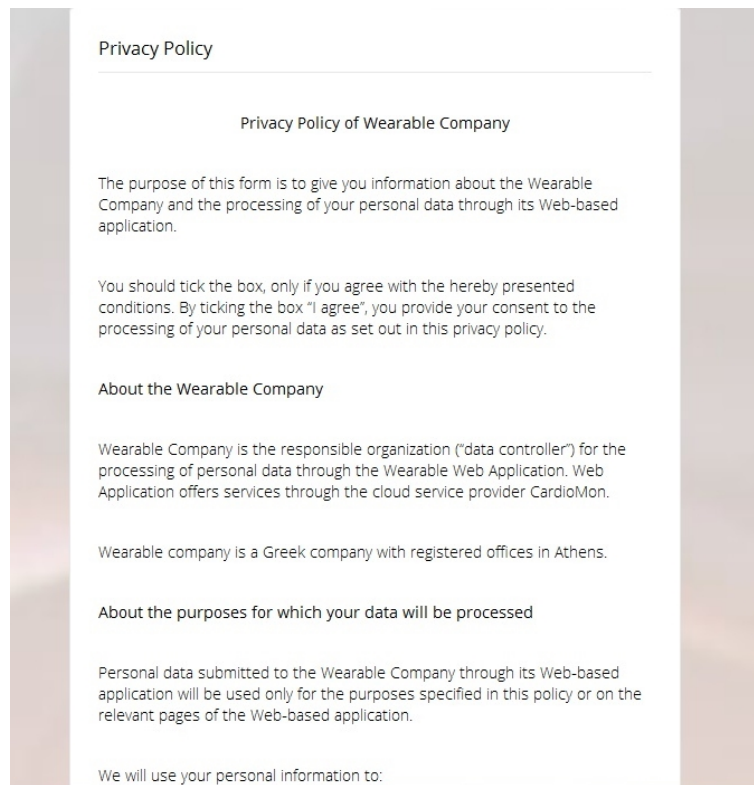
CREATE AN ACCOUNT: This section contains a paragraph of placeholder text (Lorem Ipsum) and a blue "CREATE AN ACCOUNT" button. An orange ellipse highlights the "CREATE AN ACCOUNT" button, with an orange square containing the number "1" next to it.

Figure 77: The login page of the Wearable Service.

During registration, the Wearable Co customer needs to accept a consent form on being aware of the type of personal data collected, processed and stored in this cloud service. This consent form is a compilation of the lawyer readable privacy policy and takes the form of Figure 78. After accepting this form, the wearable customer is prompted to fill in the personal data of the profile (see Figure 79), which refer to the Username, the Password, the Display Name, the Gender, the Age, the Height, the Weight and the Date of Birth and the Country of origin (the user ID is automatically assigned by the Web

³ Orange highlighted shapes (ellipses or rectangular) in solid or dashed lines are used in the screenshots to focus on a specific function on the respective Web page.

application). Using the declared credentials, the Wearable Co customer can select option 2 from Figure 77 to log in to the Web application.



The image shows a 'Privacy Policy' form for 'Wearable Company'. The form is titled 'Privacy Policy' and 'Privacy Policy of Wearable Company'. It contains the following text:

The purpose of this form is to give you information about the Wearable Company and the processing of your personal data through its Web-based application.

You should tick the box, only if you agree with the hereby presented conditions. By ticking the box "I agree", you provide your consent to the processing of your personal data as set out in this privacy policy.

About the Wearable Company

Wearable Company is the responsible organization ("data controller") for the processing of personal data through the Wearable Web Application. Web Application offers services through the cloud service provider CardioMon.

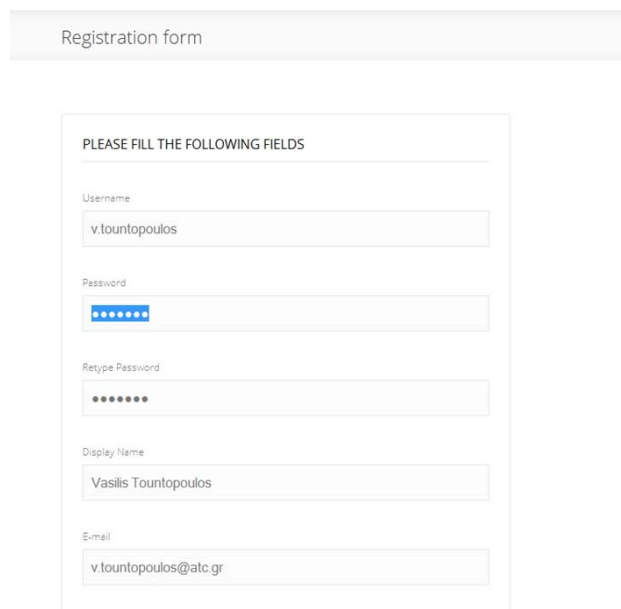
Wearable company is a Greek company with registered offices in Athens.

About the purposes for which your data will be processed

Personal data submitted to the Wearable Company through its Web-based application will be used only for the purposes specified in this policy or on the relevant pages of the Web-based application.

We will use your personal information to:

Figure 78: The consent form that the Wearable Co customer needs to accept during the registration phase.



The image shows a 'Registration form' for the 'Wearable Service'. The form is titled 'PLEASE FILL THE FOLLOWING FIELDS' and contains the following fields:

- Username: v.tountopoulos
- Password: [masked with dots]
- Retype Password: [masked with dots]
- Display Name: Vasilis Tountopoulos
- E-mail: v.tountopoulos@atc.gr

Figure 79: The Registration page of the Wearable Service

Upon successful registration and login, the Wearable Co customer is shown the screen of Figure 80. Through this page, the user either selects option 1 for real time monitoring of the collected wearable record (consisting of the attributes for the sugar level, the blood pressure and the heartbeat rate) from the wearable device or option 2 for viewing and managing the daily training activities.

Following option 1 of Figure 80, the Wearable Co customer retrieves the view of Figure 81, which displays the aggregated value of the wearable record (for each of the three attributes, namely the Sugar Level, the Blood Pressure and the Heartbeat Rate) for all the values existing in the database for this customer and normalised by a predefined threshold, representing the optimum value for each attribute. The visual representation consists of a circle, which is progressively filled in with blue colour, as the percentage value reaches 100%, while it goes to a full red coloured circle if the values exceeds 100%. Furthermore, as shown in Figure 80, the Customer can, also, request for a detailed analysis of the values for each attribute in the form of a chart, as depicted in Figure 82.

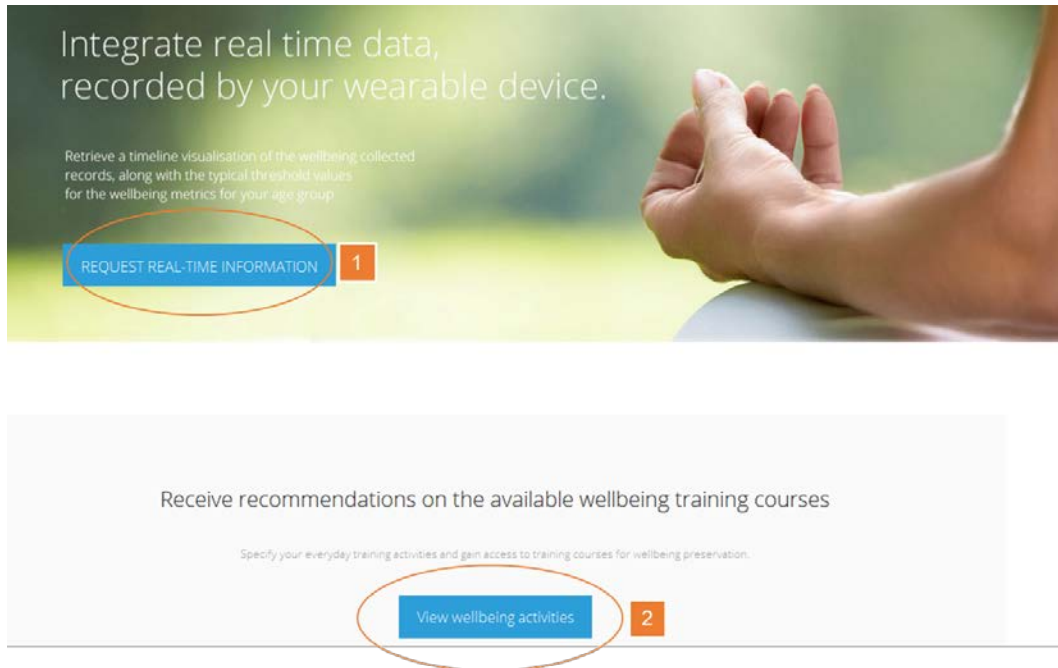


Figure 80: The first page of the logged in Wearable Customers

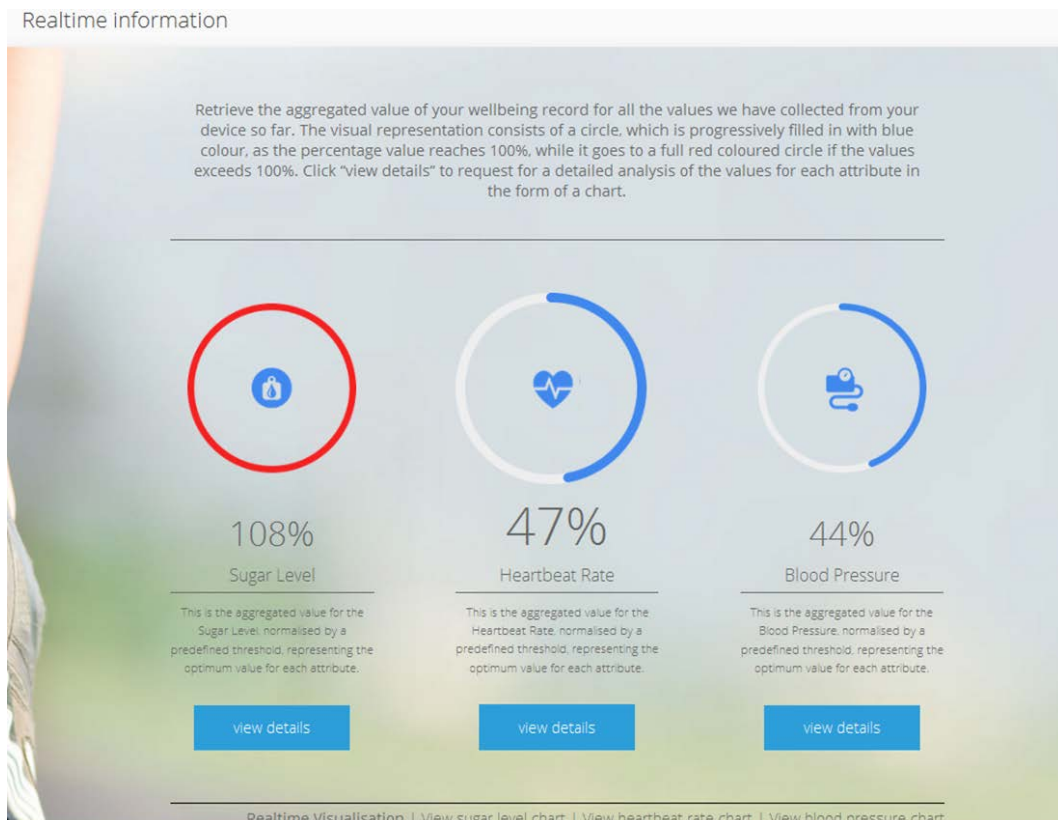


Figure 81: The real time information page of the logged in Wearable Customers



Figure 82: The Wearable Service page for chart visualisation of the real time information for the logged in Wearable Customers

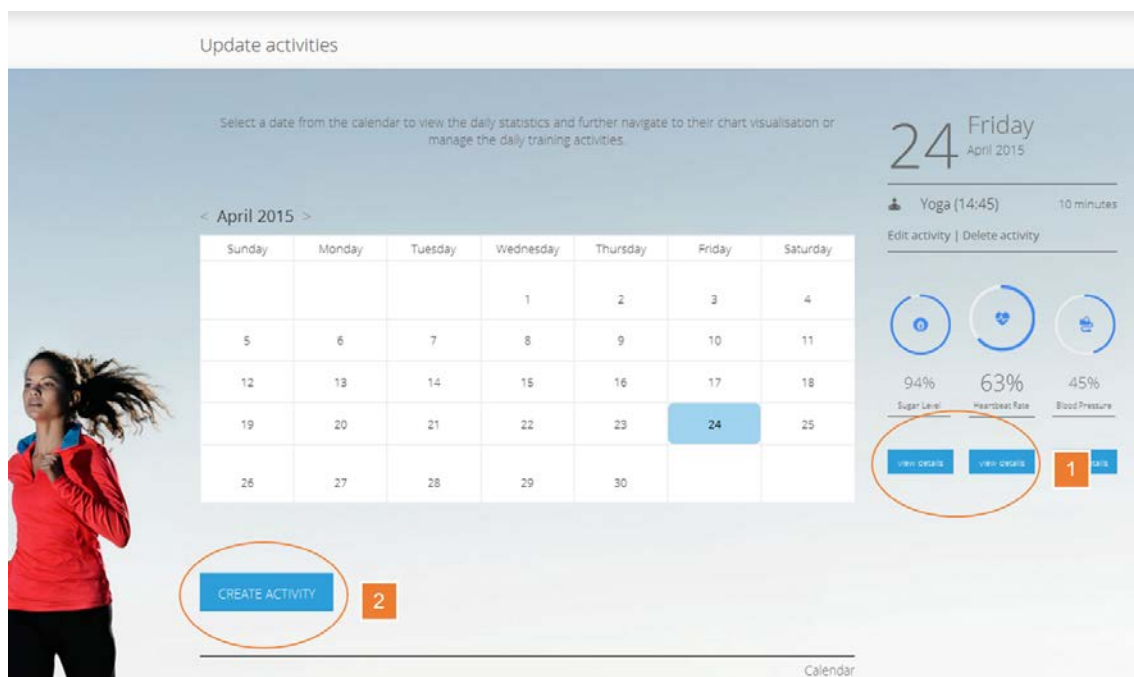
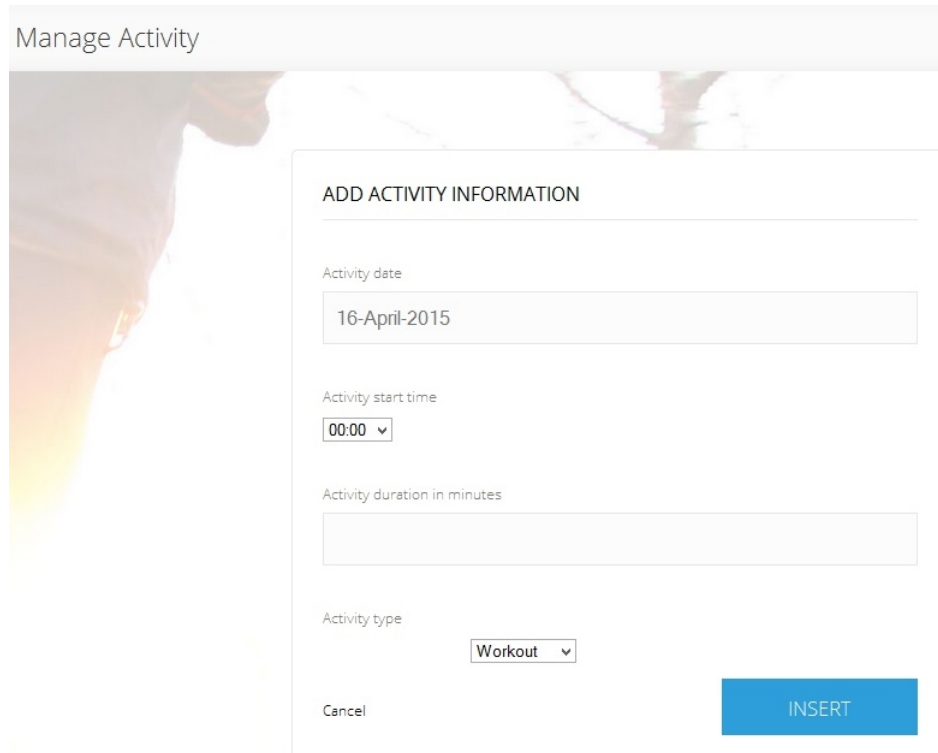


Figure 83: The screen of the Wearable Service to manage wellbeing activities

Following option 2 of Figure 80, the Wearable Co customer can manage his/her daily activities. To this end, the Web application displays the picture of Figure 83, which enables the Customer to select a date from a calendar (as shown in the middle of the picture) to populate with activities and browse the statistics of the wearable record of the current or the selected day, along with the list of daily training activities (as shown in the right hand side part of the screen). Through this view, the Customer can further navigate to the following two options:

- Option 1: select a date from the calendar to view the daily statistics and further navigate to their chart visualisation (same view as per Figure 82, but for personal data collected on the selected date), or manage the daily training activities.
- Option 2: create a new activity as per Figure 84



The screenshot shows a web interface titled "Manage Activity". It features a form with the following fields and controls:

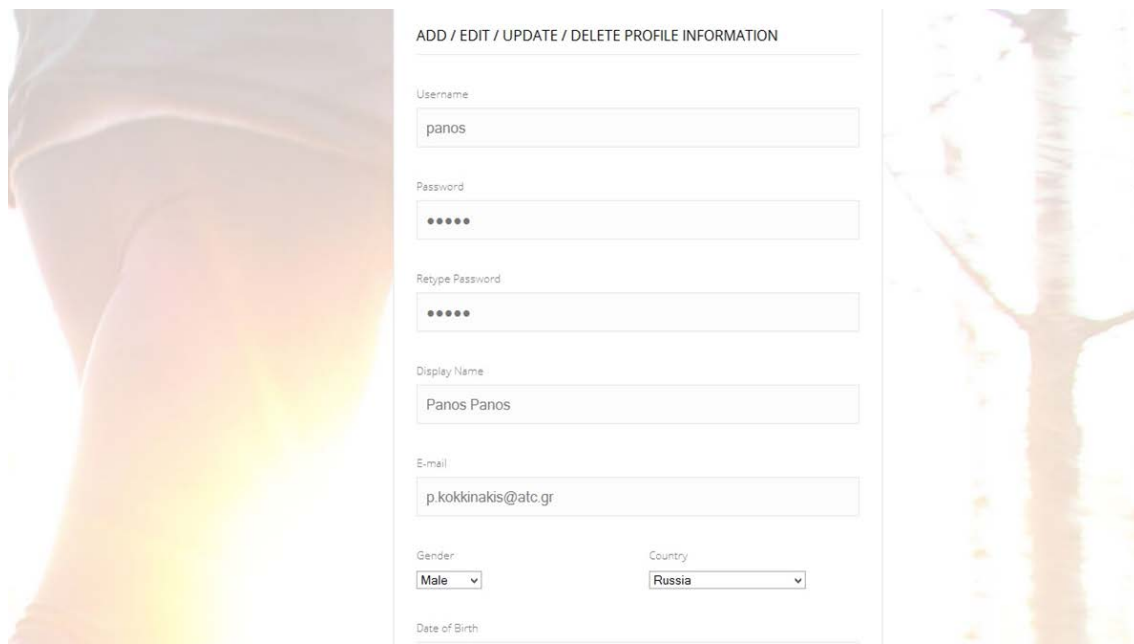
- Activity date:** A text input field containing "16-April-2015".
- Activity start time:** A dropdown menu showing "00:00".
- Activity duration in minutes:** An empty text input field.
- Activity type:** A dropdown menu showing "Workout".
- Buttons:** A "Cancel" button and a blue "INSERT" button.

The background of the form is a blurred image of a person's arm and hand.

Figure 84: Managing activities in the wearable Service

In all pages, the Wearable Co customer has access to some more pages from the menu bar on the top of the screen. From this menu and by pressing the "Profile" button, the Customer can manage and update the profile data, as shown in Figure 85.

Through the same menu bar, the Customer has access to the Statistics Page. This is an additional page, which integrates the wearable records from all the Customers registering to the Wearable Co. At this point, the request from the Wearable Service in Kardio-Mon is forwarded to the Map-on-Web side. The latter is responsible for getting the relevant information from Kardio-Mon and deliver two views: i) one similar to Figure 81, but aggregating the data coming from all the Wearable Co customers and the detailed map visualisation of Figure 86. The latter distinguishes the wearable records per country and makes the aggregation per attribute on the country level. In both cases, Map-on-Web is agnostic to the exact id of the Wearable Co customer that this data belongs to, as per the policy enforcement rules. Through, this page, neither Map-on-Web nor the specific Customer can delete any personal data.



ADD / EDIT / UPDATE / DELETE PROFILE INFORMATION

Username
panos

Password
•••••

Retype Password
•••••

Display Name
Panos Panos

E-mail
p.kokkinakis@atc.gr

Gender
Male

Country
Russia

Date of Birth

Figure 85: The Manage Profile page of the Wearable Service

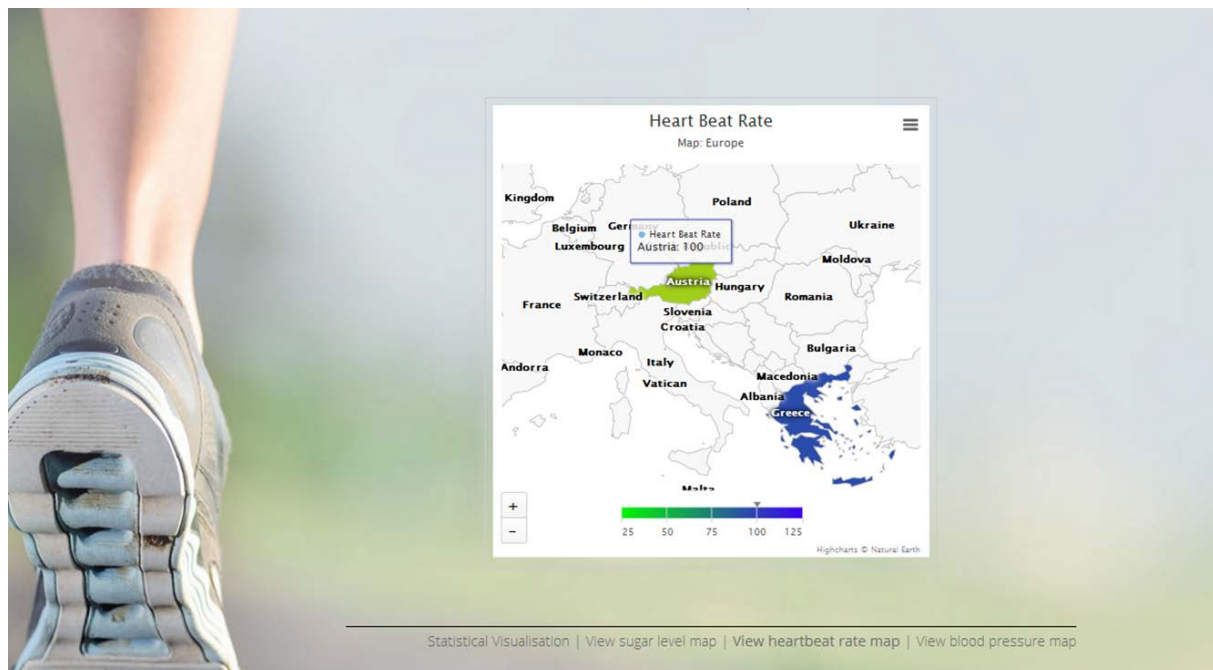


Figure 86: The statistical Map visualisation page of the Wearable Service

9.2.2 The operations of the Wearable Co Employee

The Wearable Service offers the following main pages (UI screens) for the employee of the Wearable Co, which implement the functions of **Error! Reference source not found.**:

- Log-in Page: this page enables the Employee to be authenticated to the service.
- Manage Profile page: this page enables the Employee to manage their profile data.

- Home Page: This page hosts the list of registered users to the Wearable Co and enables access to their profile.
- Customer Profile page: this page enables the Employee to browse the profile data of the selected Wearable Customer, those that the Employee has access to, according to the policy.
- Request map visualisation page: This page enables the Employee to navigate to the overall statistics of the wearable data collected from all the customers of the Wearable Service for the Wearable Co.

In the remaining part of this section we demonstrate the execution steps for this scenario of the Employee, along with a set of screenshots visualising the pages that the Employee goes through.

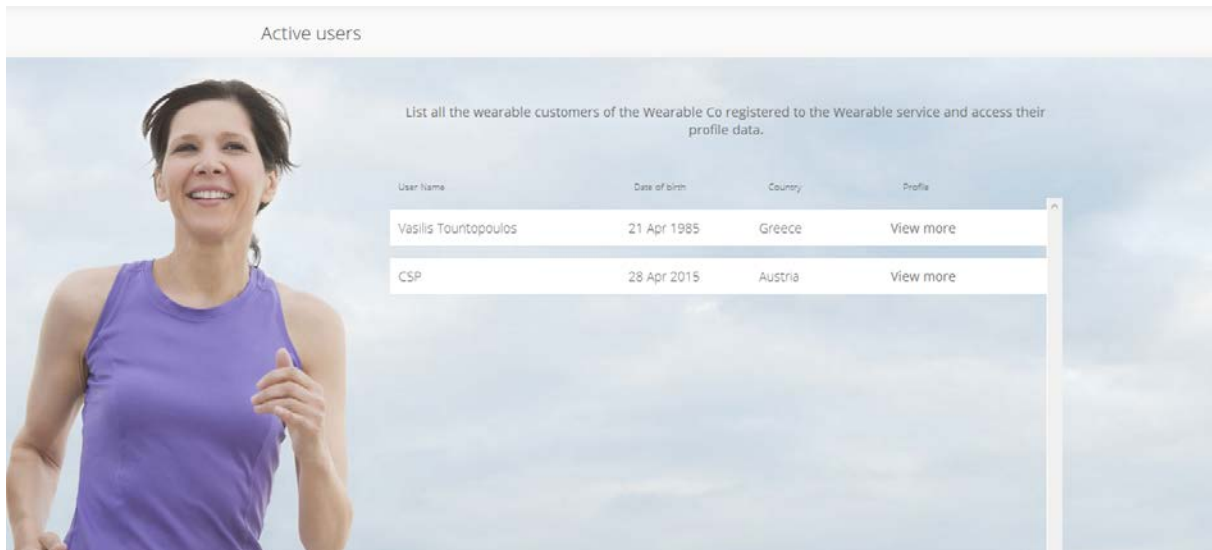


Figure 87: The first page of the logged in Employees

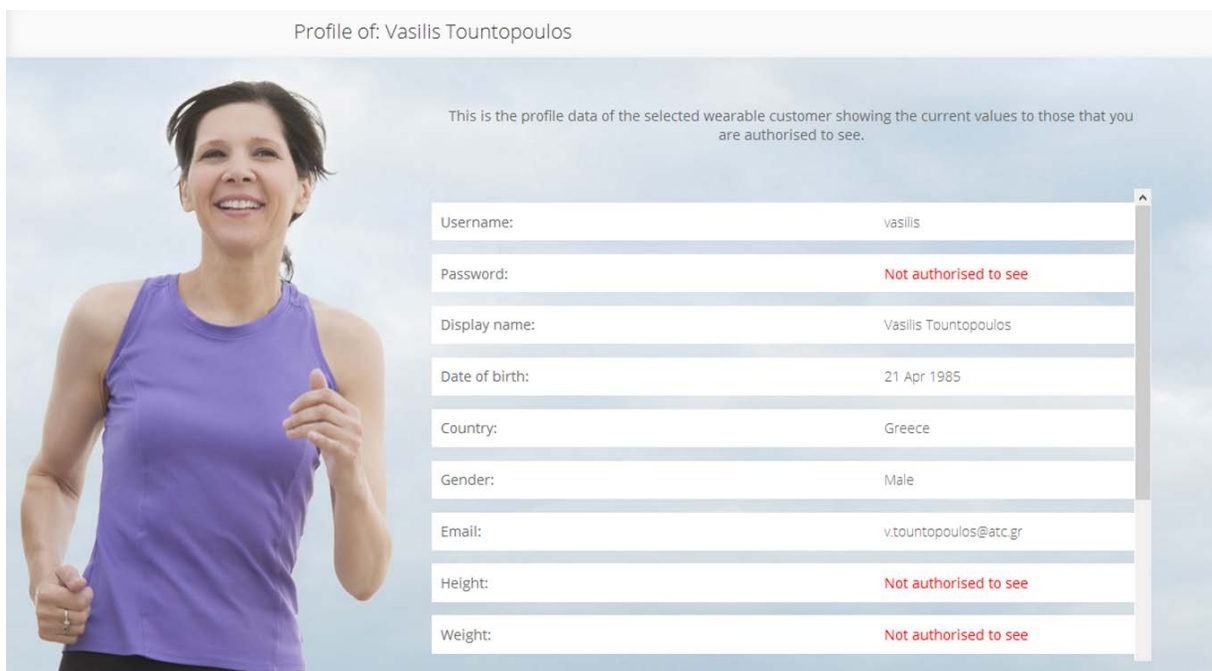


Figure 88: An employee viewing the profile of a Wearable Co customer

From the home page (see Figure 76 – shared view with the Wearable Co customer), the Employee selects the login button from the top right menu bar (highlighted by the orange dashed rectangular). The login page is then displayed, as shown in Figure 77 (shared view with the Wearable Co customer). It must be noted that the Web application assigns all the newly registered users as Wearable Co

customers and, for this prototype, we assume that the employees have pre-registered with the application beforehand.

Upon successful login to the application, the Employee is shown the screen shown in Figure 87. Through this page, the employees can browse the whole list of the Wearable Co customers can see their display name, age and country. This page, also, offers the possibility to go through the details of one customer's profile, as shown in Figure 88.

As in the case of the Wearable Co customer, through the same menu bar, the Employee has access to the Statistics Page. This is exactly the same page as for the Customers and is not explained further.

9.3 Examples of evidence records stored in AAS

9.3.1 Evidence Record Generated from A-PPLE Logs

```
<record id="1">
  <action>PII delete message@Main-Container ( 10.0.0.6) </action>
  <actor>PiiDataRetentionAgent_1042_Main-Container </actor>
  <policyID>1042</policyID>
  <supportingElements>
    <signature>
      ASWvEJSVf dMZGj 0Taff eGu3Si l 0B0bYUu+L6l oQw5k=
    </signature>
    <element xsi:type="xs:string"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      Message: PII deleted type: policy enforcement
      piiAttributeName: Country
      piiOwner: Panos
      date: 2015-12-09 10:31:43.0
    </element>
  </supportingElements>
  <supportingElements elementID="1">
    <signature>
      VCdzWj Ynz6wkAf Bt gf Srl i xUrgCl ADt +m#CnDUB7zTo=
    </signature>
    <element xsi:type="xs:string"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      Record UID: f02a600e-e69b-4cfb-9bb9-25dd911f9356
    </element>
  </supportingElements>
  <evidenceMetadata>
    <collectionInstance>
      PiiDataRetentionAgent_1042_Main-Container
    </collectionInstance>
    <evidenceDetectionTime>
      2015-12-09T10:32:02.101+01:00
    </evidenceDetectionTime>
  </evidenceMetadata>
</record>
```

9.3.2 Evidence Record Generated from OpenStack Nova Service

```

<record>
  <action>
    Snapshot Exists (1)_6b0a9a97-0ca7-4fa1-9d68-0714fe3b03c2(Kardi o-
    Mon-PII-Store) @ul (172.28.64.50,,,,,,,,,,,,,)
  </action>
  <actor>
    Pii Snapshot CheckAgent_1042_Main-Container @VAS_Core_Container
  </actor>
  <policyID>1042</policyID>
  <supportingElement selfElementID="0">
    <signature>
      qtJt gU4QzdGkD53Sqfj Qzrr898fky0Xi DbLpntUz9F8k=
    </signature>
    <element xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">
      Novalmage{id=54dd8d3e-f933-4df1-8853-f609b4bdddcc,
        name=Pii Snap, status=SAVING, progress=25, size=0,
        minRam=1024, minDisk=40, created=Wed Dec 09 10:30:35 CET
        2015, updated=Wed Dec 09 10:30:35 CET 2015,
        metadata={instance_uuid=6b0a9a97-0ca7-4fa1-9d68-
        0714fe3b03c2, instance_type_memory_mb=4096,
        user_id=d336b4929ef043c990755c67d695a1b9,
        image_type=snapshot, instance_type_id=1,
        instance_type_name=m1.medium,
        instance_type_ephemeral_gb=0,
        instance_type_rxtx_factor=1, instance_type_root_gb=40,
        instance_type_flavor_id=3, instance_type_vcpus=2,
        instance_type_swap=0, base_image_ref=a86aa4ed-5df8-4452-
        bfd0-1d6e3d872839},
        links=[GenericLink{href=http://controller:8774/v2/655bf47
        adead485fa497d9a37b1060bd/images/54dd8d3e-f933-4df1-8853-
        f609b4bdddcc, rel=self},
        GenericLink{href=http://controller:8774/655bf47adead485fa
        497d9a37b1060bd/images/54dd8d3e-f933-4df1-8853-
        f609b4bdddcc, rel=bookmark},
        GenericLink{href=http://172.28.64.50:9292/655bf47adead485
        fa497d9a37b1060bd/images/54dd8d3e-f933-4df1-8853-
        f609b4bdddcc, rel=alternate},
        type=application/vnd.openstack.image}], }
    </element>
  </supportingElement>
  <supportingElement selfElementID="1">
    <signature>
      I / QLI ZP0vr +aK4QskHTf KMPX3oDu3G6f LekM0PFQFQ=
    </signature>
    <element xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">Record UID: 353fc416-9860-40c2-a9b9-
      48e0cf530de5</element>
  </supportingElement>
  <evidenceMetadata>
    <collectionInstance>
      Pii Snapshot CheckAgent_1042_Main-Container
    </collectionInstance>
    <evidenceDetectionTime>
      2015-12-09T10:31:01.532+01:00
    </evidenceDetectionTime>
  </evidenceMetadata>
</record>

```