

---

## D:D-7.1: First system and use case prototype

---

|   |                     |
|---|---------------------|
| <b>Deliverable Number</b>                     | D47.1               |
| <b>Work Package</b>                           | WP 47               |
| <b>Version</b>                                | Final               |
| <b>Deliverable Lead Organisation</b>          | ATC                 |
| <b>Dissemination Level</b>                    | PU                  |
| <b>Contractual Date of Delivery (release)</b> | 31/01/2015          |
| <b>Date of Delivery</b>                       | 11/05/2015          |
| <b>Status</b>                                 | Free for submission |

---

### Editor

Vasilis Tountopoulos (ATC)

### Contributors

Giorgos Giotis (ATC), Pavlos Bakoulis (ATC), Richard Brown (ATC), Theofrastos Koulouris (HP), Anderson Santana de Oliveira (SAP), Thomas Ruebsamen (HFU), Rehab Alnemr (HP)

### Reviewers

Alain Pannetrat (CSA), 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 document describes the first attempt to instantiate the A4Cloud Accountability Framework, which comprises a comprehensive specification for how to create accountability for cloud services, spanning regulatory, legal, technical, business and user issues. To do so, the project offers an orchestrated set of mechanisms for addressing accountability in a preventive (mitigating risk), detective (monitoring and identifying risk and policy violation) and corrective (managing incidents and providing redress) way. In this first prototype, we emphasise on the preventive and detective mechanisms. In that respect, we showcase how the accountability framework can be applied in real life examples and we focus on the instantiation of both the framework and the accountability reference architecture in the domain of wearables.

From a technical point of view, this version of the A4Cloud prototype describes how the A4Cloud tools enable cloud providers to define, enforce and monitor policy rules in response to compliance to 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 first 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.

As previously mentioned a wearable use case has been designed to demonstrate the accountability framework and the respective tools developed by the A4Cloud project in a real life example of a cloud service chain, which exhibits certain security and privacy concerns. 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 scenario that we demonstrate in this first prototype is evolved from the perspective of the primary cloud service provider and the cloud customer. The former delivers a cloud service, which gathers, manages and stores personal data of the wearable customers in order to keep track of their long term wellbeing status. The latter (the cloud customer) is a non ICT skilled SME, which seeks a cloud provider hosting their online wearables business and enable the customers of the wearable cloud service to track their wellbeing data and visualise aggregated wellbeing statistics.

The deliverable integrates the results of the first instantiated A4Cloud prototype and reports on the knowledge transferred from the other A4Cloud WPs and the experience gained during the work of integrating the A4Cloud framework and tools in the wearable use case. Since the project envisions an interdisciplinary co-design of the Accountability Framework, this document joins up sections that can be read by various target groups, being from a legal, socio-economic or technical background.

The project officially aims for a second and final prototype of the A4Cloud instantiation to the wearables domain.

## Table of Contents

|   |    |
|---|----|
| Executive Summary .....   | 2  |
| 1 Problem Definition .....  | 5  |
| 1.1 Introduction .....  | 5  |
| 1.2 The Scope of the First Prototype .....                                  | 5  |
| 1.3 Structure.....  | 6  |
| 1.4 Glossary of Acronyms / Abbreviations .....                              | 6  |
| 2 Specifications of the Wearable Use Case.....                              | 8  |
| 2.1 The Storyboard of the Use Case .....                                    | 8  |
| 2.2 Updated Definition of the Wearable Service .....                        | 10 |
| 2.3 Introduction to the Accountability Phases of the Wearable Service ..... | 14 |
| 3 Integration of the A4Cloud Components .....                               | 20 |
| 3.1 Instantiation of the Cloud Accountability Reference Architecture .....  | 20 |
| 3.2 Physical Deployment of the A4Cloud First Prototype .....                | 23 |
| 3.3 Guidelines for Use Case Developers.....                                 | 26 |
| 3.3.1 Policy Definition and Compliance.....                                 | 27 |
| 3.3.2 Policy Enforcement .....  | 31 |
| 3.3.3 Collection & management of evidence.....                              | 33 |
| 3.3.4 Data Subject Enablement.....  | 36 |
| 3.3.5 Notification and Remediation .....                                    | 36 |
| 4 Presentation of the Wearable Use Case.....                                | 38 |
| 4.1 The history of the scenario.....  | 38 |
| 4.2 Analysing and designing the Wearable Service .....                      | 39 |
| 4.2.1 The perspective of CardioMon .....                                    | 39 |
| 4.2.2 The perspective of the Wearable Co.....                               | 46 |
| 4.2.3 Implementation of Measures .....                                      | 48 |
| 4.3 Operating the Wearable Service.....                                     | 52 |
| 4.3.1 The operations of the Wearable Customer .....                         | 53 |
| 4.3.2 The operations of the Wearable Co Employee .....                      | 59 |
| 4.4 Gathering Evidence.....   | 61 |
| 4.5 Handling Exceptions .....   | 62 |
| 4.6 External Verification .....   | 63 |
| 5 Overview of the User Engagement and Evaluation Planning .....             | 67 |
| 5.1 Overview of the Methodology .....                                       | 67 |
| 5.2 The dimensions of the evaluation methodology .....                      | 68 |
| 5.3 The Evaluation Audience .....   | 69 |
| 5.4 The Evaluation Tools .....  | 70 |
| 5.5 Engagement towards evaluation.....                                      | 70 |

|        |  |     |
|--------|--|-----|
| 6      | Conclusions .....  | 71  |
| 7      | References .....   | 71  |
| 8      | Appendices .....   | 72  |
| 8.1    | Aspects of the Use Case Development .....                                  | 72  |
| 8.1.1  | Registration Service .....   | 72  |
| 8.1.2  | Update PII .....   | 73  |
| 8.1.3  | Request Real-time information: Histogram Visualisation .....               | 73  |
| 8.1.4  | Request Real-time information: Average Values .....                        | 74  |
| 8.1.5  | View activities: Wellbeing statistics .....                                | 74  |
| 8.1.6  | View activities: Get activities on date .....                              | 74  |
| 8.1.7  | Active users .....   | 75  |
| 8.1.8  | Statistics .....   | 76  |
| 8.1.9  | Map Visualisation .....  | 76  |
| 8.1.10 | Alert messages .....   | 76  |
| 8.1.11 | Get PII all .....  | 76  |
| 8.1.12 | Delete PII all .....   | 77  |
| 8.2    | The high level legal and normative obligations of the use case roles ..... | 78  |
| 8.3    | The Lawyer Readable Privacy Policy .....                                   | 81  |
| 8.4    | The machine readable accountability policy .....                           | 83  |
| 8.5    | Machine readable policy for DTMT configuration .....                       | 97  |
| 9      | Index of figures .....   | 99  |
| 10     | Index of tables .....  | 100 |

## 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 corporate and private 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 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 a toolset, which aims to support the implementation of these mechanisms. The tools comprising this toolset 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 toolset 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.

In that respect, this deliverable is the report following the prototype implementation of the first instantiation of the A4Cloud accountability framework and the toolset in real life examples. As explained in [2], we have selected the wearables domain and relevant use case scenarios from it to demonstrate the effectiveness of the framework and the applicability of the tools to address the accountability concerns raised in this use case.

### 1.2 The Scope of the First Prototype

In this first prototype, we present the specifications of the wearable 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 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 coverage of the first prototype lays on the preventive and detective mechanisms and corresponding tools. As such, this deliverable integrates the outcome of the Contract and Risk Management functional area into the analysis phase of the accountability lifecycle processes, which drives the identification of legal and normative obligations and the specification of relevant accountability policies. The latter are, currently, built manually, but the document tries to integrate the knowledge from multi-disciplinary business executives, namely legal, socio-economic and technical experts. The deliverable shows how these policies are enforced in various places within the cloud environment, set up for the purposes of the wearable use case, and describes the processes for the collection of evidence from the runtime execution of the wearable service. Emphasis is given on the detection of various incidents, which is performed with the support of the A4Cloud tools. Finally, the first prototype includes steps for the internal and external verification of the supported data handling processes, through audits.

Although this document summarises the activities with respect to the first A4Cloud prototype, the document tries to map the complete specifications of the final prototype as well, by incorporating those steps, which have not yet been integrated through manual steps in the process (for example the manual

deployment of accountability measures). The goal is to offer insight about the full picture of the accountability support in this use case, even at this stage of development.

### 1.3 Structure

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

- Section 2 presents the business dimension of the wearable use case, by elaborating on the story, which is evolved around this use case. It introduces the various roles in the operational scenario and defines the specifications for the target cloud-based environment, under study, which is the wearable service. It, then, presents an overview of the operations within the wearable service, as seen from an accountability point of view. The information provided in this Section should be accessible to all readers of this deliverable.
- Section 3 analyses the technical aspects of the first prototype. Starting from the Accountability Reference Architecture, the section elaborates on the different aspects of this architecture, such as the accountability support services, and provides guidelines for developers on how they can adopt the Accountability Framework to build their own application from an accountability perspective. This section mainly targets readers with a technical background, thus it, also, presents the physical deployment of the A4Cloud First Prototype for the wearable use case.
- Section 4 is the core part of the first instantiated A4Cloud prototype. This section starts with the history of the demonstration scenario and, then, elaborates the various aspects of the accountability instantiated framework and tools for the analysis, design and operation of the cloud-based Wearable Service. The presentation of the first prototype is unfolded around the Accountability Lifecycle steps. As such, we select the most suitable time slots of the scenario to make emphasis on the perspective of the key roles for this version of the prototype in the application of the framework and the tools. In that respect, the demonstration is presented from the perspectives of the primary cloud service provider (CardioMon) and the cloud customer (the Wearable Co). Since this section is the mirror of the work performed in WP47 so far, this section reflects the requirements of all the readers.
- Section 5 describes the plan for the evaluation of the A4Cloud work in the context of the wearable use case. Thus, it analyses the objectives of the user validation tasks and the process to be followed in order for the appropriate stakeholders to be engaged in the user evaluation phase .
- Finally, Section 6 concludes this deliverable and provides the link to future work.

### 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         |
| AT                     | Assertion Tool                              |
| CARA                   | Cloud Accountability Reference Architecture |
| CEO                    | Chief Executive Officer                     |
| COAT                   | Cloud Offerings Advisory Tool               |
| DPIAT                  | Data Protection Impact Assessment Tool      |
| DT                     | Data Track                                  |
| DTMT                   | Data Transfer Monitoring Tool               |
| IaaS                   | Infrastructure-as-a-Service                 |

| Acronym /<br>Abbreviation | Description                                |
|---------------------------|--|
| IMT                       | Incident Management Tool                   |
| PaaS                      | Platform-as-a-Service                      |
| PAPV                      | Plug-in for Assessment of Policy Violation |
| PII                       | Personally Identifiable Information        |
| PLA                       | Privacy Level Agreement                    |
| PO                        | Privacy Officer                            |
| RRT                       | Remediation and Redress Tool               |
| SaaS                      | Software-as-a-Service                      |
| SME                       | Small-Medium Enterprise                    |
| TL                        | Transparency Log                           |
| UI                        | User Interface                             |

## 2 Specifications of the Wearable Use Case

The Wearable Use Case has been designed to demonstrate the accountability framework and the respective tools developed by the A4Cloud project in a real world example of a cloud service supply chain. This use case constitutes a realistic and topical scenario, in which the involved business actors have to take the appropriate actions to ensure that the collection and processing of the customers' personal data are handled responsibly, based on the established regulations and declared security organisational policies.

The specifications of this scenario aim to cover the complete accountability life cycle for the involved actors, in order to deliver the service envisioned in the Wearable Use Case (the Wearable Service). In that respect, the scenario is constructed from the perspective of the cloud customer, who aims to build a Web-based application for offering well-being data analytics services to its customers. In order to do so, this cloud customer needs to carefully select the cloud provider(s), who will provide the respective cloud environment to host this application and the supporting services involved. The application integrates various functionalities, which require the collaboration of different cloud providers in the background. As such, the selection process should consider the implications of potential third parties' engagement in the provision of the Wearable Service, who should prove their commitment to the legal framework and their customers' preferences, with respect to the personal and business confidential data made available to them for processing (i.e. access, analysis, management, storage, etc.).

In order to draw the boundaries of the first instantiated prototype of the Wearable Use Case, in this deliverable we focus on the accountability interactions that happen between the following actors in specific accountability interaction paths, namely agreement, reporting, demonstration and remediation, as they are introduced in [3]:

- The Cloud Subjects, who are the customers of a company offering a service which utilises cloud resources (Cloud Customer). A Cloud Subject and the Cloud Customer interact with each other, during the following accountability paths: agreement, reporting and demonstration.
- The Cloud Customer, who establishes a business relationship with a Cloud Provider for processing personal data and business confidential information as part of its service provision. These actors interact during the following accountability paths: agreement, reporting and demonstration.
- The Cloud Provider, who on its own or in collaboration with other Cloud Providers provides the necessary resources for processing personal data and business confidential information. These actors interact during the following accountability paths: agreement, reporting and demonstration.
- The Cloud Auditors and Supervisory Authorities, who are responsible for performing external verification and compliance checks towards cloud providers and customers. These actors interact during the demonstration accountability path.

In this first prototype, we eliminate the interactions referring to the demonstration of compliance between the Cloud Customer and Providers to the Cloud Auditor in case of policy violations, while the respective demonstration of compliance to policy specifications is left for the final prototype. We, also, leave the demonstration of the corrective accountability mechanisms and the implementation of the remediation interaction path for the final instantiated prototype. However, the description of the use case in this section addresses the requirements of the both the first and the final instantiation.

### 2.1 The Storyboard of the Use Case

The Wearable Co is an SME company, established in Greece, which aims to enter the wellbeing market by offering innovative products and services to address the needs of the general public. The business will initially target Greece and other European Union Member States. The Wearable Co manufactures wearable devices, which are offered to customers on a fee-basis and collect real time data for them, such as heartbeat rate, number of steps walked and blood pressure, etc. The company wants to support the business of selling physical devices by packaging them with value-added software services that collect personal data (both static/profile and dynamic real-time data) off the wearable devices, store, analyse and visualise them to make personalised reports on the wellbeing status of the device users and recommendations on preserving a wellbeing attitude. As such, the Wearable Co devices expose a



communication interface to remotely deliver and monitor data to an external storage and processing space.

The Wearable Co, as a traditional manufacturer of hardware devices lacks the appropriate resources and know-how to develop and support innovative wellbeing software applications on their own. Firstly, due to the envisaged big data volume and the lack of supporting infrastructure, the Wearable Co has to engage an Infrastructure-as-a-Service (IaaS) Provider to host the vast amount of data collected from the wearable devices. Additionally, as a non-ICT company, the Wearable Co has to rely on one or more third parties to implement the systems responsible for receiving the data exposed by the wearable devices, storing them in the cloud infrastructure and making the wellbeing recommendations available through a Web application, which is the Wearable Service. However, the engagement of third parties and the need for a cloud deployment of the Wearable Service raises concerns on whether the collaborating cloud providers are accountable organisations to ensure the security and privacy of both the personal data gathered from the wellbeing customers and the business information for issuing the wellbeing recommendation, which is confidential.

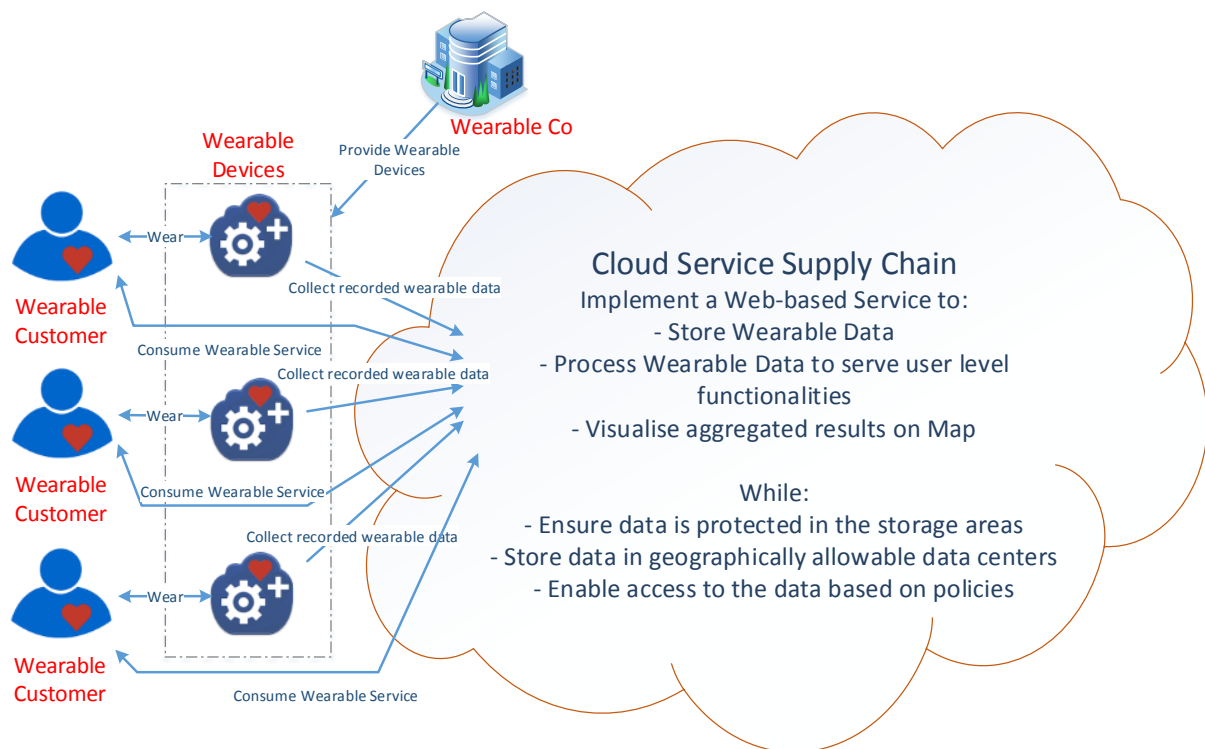


Figure 1: The conceptualisation of the Wearable Service

Figure 1 presents the concept of the Wearable Service. As shown there, the Wearable Co, as the manufacturer of the wearable devices, needs to select a cloud provider to build a Web-based service, on their behalf. This service should facilitate the processing and storing of wearable data and providing user level functionalities, which will be consumed by the wearable customers via a Web User Interface (UI). The Wearable data will be collected following two ways: i) automatic collection via the wearable device and ii) manual input from the customer via the Web application. Part of the application will involve the visualisation of aggregated statistics on maps. It should be noted that the service should be realised through one or more cloud service providers (the cloud service supply chain).

As shown in Figure 1, the Wearable Co may raise some concerns with respect to the implementation of the Wearable Service in the cloud. These concerns are driven by the legal framework and the type of personal data that should be collected. In this case, the Wearable Co should ensure that all the personal data collected by the wearable customers (either automatically or manually) is protected at all phases on their processing, while a specific set of geographical data centres should be considered for storing. At the same time, this SME should apply specific data access and data handling rules that should be enforced at runtime by all the involved stakeholders in this Wearable Service.

We now consider CardioMon, which is a Software-as-a-Service (SaaS) cloud provider offering a complete solution in the wellbeing domain, by means of providing features for collecting, managing, storing and processing wellbeing data. CardioMon is doing business with many other customers with similar functional / business requirements as Wearable Co and has an existing business agreement with DataSpacer, an IaaS Cloud Provider, who offers advanced security and privacy mechanisms (such as data access groups, data encryption, etc.) for the protected storage and processing of personal and sensitive information. Furthermore, the CardioMon service allows for the core functionality to be expanded via third-party services to enrich the experience of the wellbeing users. Such an expansion is provided by Map-on-Web, which is a separate SaaS cloud provider, with expertise in map visualisations for big data sets. Thus, Map-on-Web complements CardioMon by expanding the available data visualisation features.

The scenario of this use case assumes that (after a period of researching the market) Wearable Co selects CardioMon as the provider of the software service that it will make available to its customers. Implementing the outcomes of the A4Cloud project, the Wearable Co adopts an accountability-based approach over how the data collected about the customers are handled and processed. This involves the establishment of a policy agreement with CardioMon, who, in turn, will be responsible for protecting the customers' personal data and the Wearable Co confidential information, which is disclosed to CardioMon in order to facilitate the provision of the desired functionalities. This policy involves rules and conditions with respect to data handling practices. CardioMon is responsible for enforcing the policy in their interactions with both the Cloud subjects (the Wearable Customers) and the providers (Map-on-Web and DataSpacer).

At the same time, the corresponding cloud providers are assumed to have already implemented the accountability tools and other mechanisms of the A4Cloud project for their own part, being accountable to their collaborating providers. For example, CardioMon agrees with Map-on-Web on specific accountability policies with respect to how the aggregated data of the Wearable Customers are processed by the Map-on-Web service to offer the requested map visualisations. A4Cloud supports the definition and enforcement of these policies on both providers, so that Map-on-Web is accountable to CardioMon for the way that the aggregated data of the Wearable Customers are processed to produce the map visualisations, while CardioMon is accountable to the Wearable Co for the conditions under which the Map-on-Web, as a third party, accesses this personal data.

This will enable the operators of the Wearable Service to act in an accountable manner and be compliant to certain legal requirements. However, within the service lifetime, policy violation and security and privacy incidents are likely to occur, which set the Wearable Service vulnerable to accountability related inconsistencies. The latter can originate either from an abnormal operation undertaken by any actor in this use case or a security or privacy related failure in the cloud service supply chain itself. Thus, A4Cloud tools assist CardioMon, for example, in detecting an incident raised by either a policy violation or a security/privacy breach. CardioMon, subsequently, has to remedy the incident, according to the provisions of the policy and mitigate the risk arising from this incident. The same applies for the other cloud providers. In this sense, DataSpacer is hosting the relevant A4Cloud tools, which are monitoring DataSpacer actions and raise an alert about a data transfer action that could potentially be a policy violation.

Based on this storyboard, in the next section, we elaborate on the definition of the Wearable Service.

## 2.2 Updated Definition of the Wearable Service

In Section 2.1, we elaborated on the storyboard for the Wearable Service and the expected high level overview of the actions to be taken by the identified actors **for this first prototype**. In this section, we elaborate on the definition of the Wearable Service, by extending the specifications of this scenario, as they have already been introduced in the A4Cloud Deliverable D:B-3.2 [2]. In order to do so, we build on the main objective of the Wearable Service, which is to gather, manage and store personal data of the wearable users to keep track of their health status over time for long wellbeing preservation. The wellbeing related information integrates real time data that are recorded by the wearable devices provided by the Wearable Co and transmitted through the communication interface of these devices to CardioMon. The latter implements certain security and privacy preserving mechanisms to share part of this information with Map-On-Web and serve the wearable customers with a Web 2.0 application, which

enables them to consult their wellbeing data, receive wellbeing recommendations and visualise aggregated wellbeing statistics on interactive maps.

Figure 2 shows an overview of the Wearable Service, which is the implementation of Figure 1 for the selected cloud service supply chain. Consequently, in this figure, we depict the cloud environment, consisting of the respective service and infrastructure providers that serve the Wearable Service and the actors that will operate and consume this application. As such, the figure presents the relationship between these actors and the flow of the information in order to deliver the Wearable Service to the appointed customers.

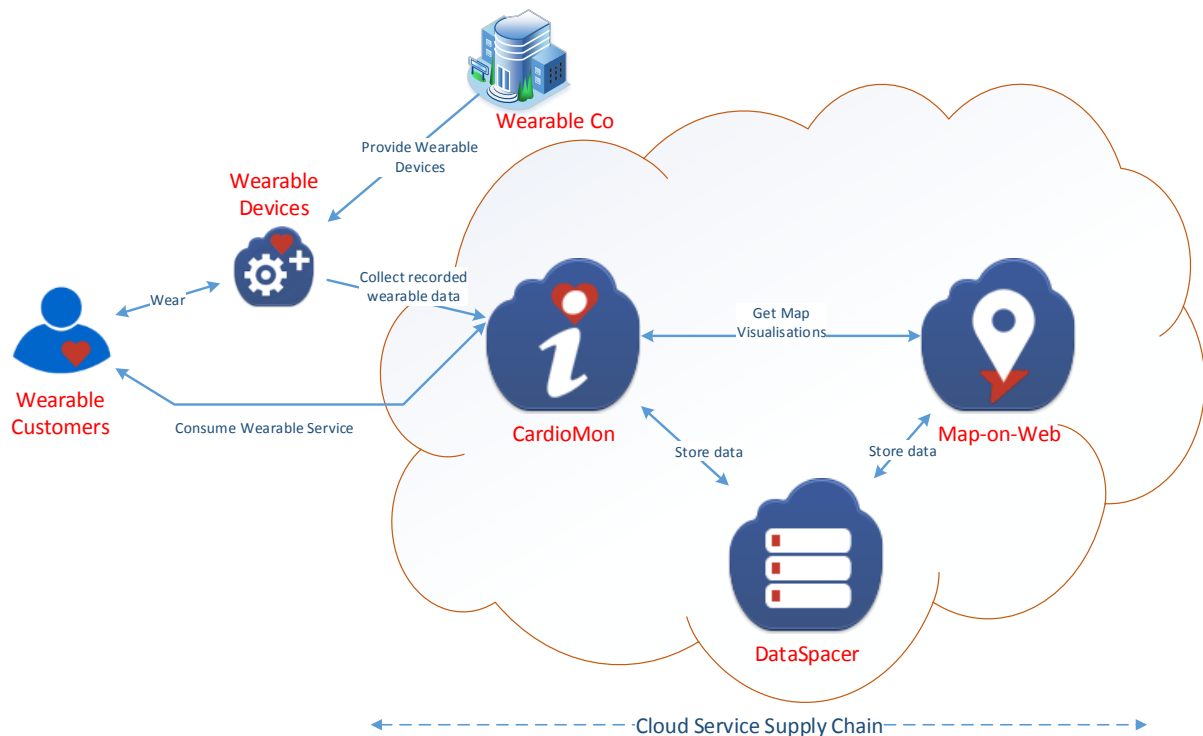


Figure 2: The use case overview for the Wearable Service – the Business Perspective

As it can be seen from Figure 2, the Wearable Co, as an SME, aims to offer an application (the Wearable Service) and, to this direction, it utilises the cloud by offering its customers a Web-based application that will enable them to control the data collected by the wearable devices (operated by the Wearable Co) and get customisable visualisations of their wellbeing status. The Wearable Service is supported by the cloud service chain depicted in this Figure 2. As stated in Section 2.1 and shown in Figure 2, CardioMon is the primary cloud service provider, which establishes a business relationship with the Wearable Co, acting as the interaction point between the cloud service supply chain and the cloud customers. In the back end, this supply chain is implemented through the collaboration of CardioMon with Map-on-Web and DataSpacer to serve additional functionalities.

In this respect, the Wearable Customers maintain two different data streams with the Wearable Service. The first one goes through their devices to CardioMon in order to automatically push wellbeing data to the cloud. In the second flow, the Wearable Customers subscribe to the Web Application offered by CardioMon and being operated by the Wearable Co to gain access to the respective wellbeing functionalities. In both cases, a matter of major concern from a data protection perspective is the way that the customers are informed of the obligations and the data handling procedures of Wearable Co, in order to give their consent for their personal data collection and processing. For example, upon registration to the Web-based cloud application, a customer profile is created, which is used by the service to continuously provide the customer with visualisations of his/her data, according to the analysis of his/her daily body measures. The registration process involves the customers giving their consent regarding the collection of their data by the devices and their handling by CardioMon and the Wearable Co, as well as any involved third party providers. The customers (Cloud Subjects) are then authorised

to interact with the service and use the suggested wellbeing programs, while, at a later point in time, they can further request an analysis of their wellbeing status, based on historical records.

At this stage of design, the Wearable Service offers a set of functionalities, which aim to satisfy the needs of the Wearable Customers on preserving a wellbeing life style, through their daily exercise. In that respect the Wearable Service offers the functionalities shown in Table 1.

*Table 1: The user level functionalities of the Wearable Service*

| ID  | Title of Functionality                       | Description   | Used by                                  |
|-----|--|---|--|
| F1  | Create Customer Profile                      | Create a customer account to the Wearable Service, by determining the credentials for logging into the service and providing profile data to be processed by the service  | Wearable Customer                        |
| F2  | Create Business User Profile                 | Create an account for managing the users registered to the Wearable Service and retrieving information about their public data submitted to the service   | Wearable Co employee                     |
| F3  | Log in                                       | Provide the security mechanism for the user authentication to the service   | Wearable Customer / Wearable Co employee |
| F4  | Manage Profile                               | Add / edit / update / delete profile information  | Wearable Customer / Wearable Co employee |
| F5  | Submit Real-time Information                 | Upload data stream with the recorded wellbeing information per time unit (e.g. per hour or per day) as collected by wearable device. Such data involve the heart beat rate, the blood pressure, the sugar blood level, etc. These data are associated with the current geographical position of the user. | Wearable Customer                        |
| F6  | Request Real-time Information                | Retrieve a timeline visualisation of the wellbeing collected records, along with the typical threshold values for the wellbeing metrics per age group and country (for the specific customer)   | Wearable Customer                        |
| F7  | Update Wellbeing activities                  | Specify everyday activities (such as the duration of a running / walking exercise, etc.)  | Wearable Customer                        |
| F8  | Get wellbeing training                       | Receive recommendations on the available wellbeing training courses   | Wearable Customer                        |
| F9  | Get wellbeing score                          | Receive a single value wellbeing score by combining information from the collected real time information and wellbeing training activities.   | Wearable Customer                        |
| F10 | Manage Business Formula for wellbeing scores | Define the thresholds (per real time data stream, e.g. blood pressure, per age and country) and the weights, through which the wellbeing score of a customer is determined  | Wearable Co employee                     |
| F11 | Update Thresholds                            | Update the threshold for the acceptable values of the wellbeing metrics, possibly customised to   | Wearable Co employee                     |

| ID  | Title of Functionality                       | Description   | Used by                                  |
|-----|--|---|--|
|     |  | geographical locations (affected by climate and altitude factors)   |  |
| F12 | View active users                            | Browse through the list of registered users and part of their profile data  | Wearable Co employee                     |
| F13 | Request Statistical Visualisation            | Get a map visualisation of the anonymised wellbeing record data (i.e. blood pressure, accountability score, etc.) per country and age group   | Wearable Customer / Wearable Co employee |
| F14 | Request data handling compliance             | Get an audit report on how data involved in the Wearable Service are handled in the cloud, by presenting relevant evidences, such as access logs and listing access violations (if any) | Wearable Co employee                     |
| F15 | Request data disclosure path                 | Get a summary of the personal data that the Wearable Service is processing for the specific Wearable Customer   | Wearable Customer                        |
| F16 | Receive alerts on excessive wellbeing values | In cases of human body metrics getting exceptional (beyond thresholds) values, raise notifications to the referred user   | Wearable Customer                        |
| F17 | Receive policy violation alert               | Receive a notification on the type of policy violation and detailed information about it  | Wearable Customer / Wearable Co employee |
| F18 | Receive transfer violation alert             | Receive a notification on the detailed data transfer violation  | Wearable Customer / Wearable Co employee |
| F19 | Receive breach notification                  | Receive security and/or privacy breach notifications  | Wearable Customer / Wearable Co employee |

These functionalities depict the actions that should be taken by the target end users to consume the results of the Wearable Service through the available functions of the front-end User Interface. In the back end, the data produced or consumed by the Wearable Customer and the Wearable Co are processed by the respective cloud providers, namely CardioMon, Map-on-Web and DataSpacer. CardioMon is the primary cloud service provider in the supply chain and the one that has been appointed by the Wearable Co to serve the functionalities offered by the Wearable Service. As such, CardioMon is the primary receiver of the accountability obligations that dictate the responsibilities undertaken by this actor to deliver a secure and privacy friendly cloud environment.

Through the available interfaces, CardioMon builds the wellbeing profile of the customers, consisting of personally identifiable information (PII). For this use case, it is considered that some data are publicly available and can be viewed by more actors than the data subjects, whereas some others are considered sensitive. By sensitive data, we mean all these private data, access to which is allowed only to the data subjects and those actors that have rights to process them, according to the policies. The classification of data types is summarised in Table 2. It must be noted that the assignment of data to data types in this Table is just an example adopted for this deliverable.

Table 2: Type of data comprising the wellbeing profile

| Data Name       | Data Description  | Type of Data  |
|-----------------|---|---------------|
| <b>Username</b> | The username used as user credentials, along with the password, to log in to the Wearable Service | Sensitive PII |



| Data Name                | Data Description   | Type of Data  |
|--------------------------|--|---------------|
| <b>Password</b>          | The password used as user credentials, along with the username, to log in to the Wearable Service  | Sensitive PII |
| <b>User ID</b>           | The unique identification number assigned to the user in order to accomplish user specific actions within a session life time  | Sensitive PII |
| <b>Display Name</b>      | The nickname selected by the user to display on the Wearable Service front end, as a comprehensive user reference  | Public PII    |
| <b>Gender</b>            | 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 PII    |
| <b>Age</b>               | 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 PII    |
| <b>Height</b>            | The height of the user to be used for determining wellbeing related information by joining up the wellbeing record with the body type.   | Sensitive PII |
| <b>Weight</b>            | The weight of the user to be used for determining wellbeing related information by joining up the wellbeing record with the body type.   | Sensitive PII |
| <b>Sugar Level</b>       | The sugar level in the user's blood, measured by the wearable device   | Sensitive PII |
| <b>Blood Pressure</b>    | The user's blood pressure, measured by the wearable device   | Sensitive PII |
| <b>Heartbeat Rate</b>    | The user's heart beat rate, measured by the wearable device  | Sensitive PII |
| <b>Training Activity</b> | The daily exercises taken by the user, such as time of walking, running, swimming and any other physical exercise  | Sensitive PII |
| <b>Wellbeing Score</b>   | The value of the wellbeing score, based on the formula defined by the cloud service  | Sensitive PII |
| <b>Country</b>           | The country of permanent residence of the user   | Public PII    |

### 2.3 Introduction to the Accountability Phases of the Wearable Service

In order to examine this use case from an accountability perspective, we first provide a holistic view on how the different roles involved in the scenario depicted in Figure 2 should collaborate in the various functional elements of the accountability lifecycle by implementing respective preventive, detective and corrective accountability mechanisms. In order to implement these mechanisms in the context of the accountability lifecycle, we first need to consider the cloud computing and data protection role assigned to each actor of the use case.

The role assignment strongly refers to perspective, from which the accountability lifecycle is considered and the time scale of the use case. For example, at the time that CardioMon wants to find appropriate cloud providers to set up the Wearable Service, this actor is a Data Controller. In this sense, Table 3 presents the assignment of the actors to roles with focus on the time that the Wearable Co wants to buy an instance of the Wearable Service. In this case, the Wearable Co acts as a Data Controller.

*Table 3: 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 Customer      | The end user of the Wearable Service   | Individual Cloud Subject      | Data Subject         |
| Wearable Co            | The SME operating the Wearable Service   | Organisational Cloud Customer | Data Controller      |
| CardioMon              | A SaaS SME cloud provider offering the Wearable Service  | Cloud Provider                | Data Processor       |
| Map-on-Web             | A SaaS cloud provider allowing the creation of maps overlaid with annotated itineraries, based on annotated GPX traces   | 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       |

Figure 3 recalls the functional elements of the accountability lifecycle as they have been introduced in the A4Cloud Deliverable D:C-2.1 “Conceptual Framework”. Based on this figure, the instantiation of the use case should demonstrate how the different actors involved the scenario follow these functional elements and adopt and perform the accountability practices, which are implemented through respective mechanisms.

In order to realise how the Accountability framework is instantiated for this Wearable Service, we, first, need to consider from which actor perspective we follow the evolution and execution of the accountability processes. To this end, the role of the data controller (the Wearable Co in our case) could be the starting point. However, due to the nature of the wearable scenario, it would be appropriate to assume the perspective of CardioMon as well, since this is the actor running a specific instance of the Wearable Service on behalf of the Wearable Co. Thus, the presentation of the accountability elements for the Wearable Service emphasise on the role of CardioMon in the execution of this use case, while, in Section 4, we put the perspective of the Wearable Co into the picture. It must be clarified, though, that the functional elements of the accountability lifecycle depicted in Figure 3 should be followed by all the cloud providers in this use case, depending on the timing of the use case scenario execution and their involvement and/or contribution to the development of the cloud service supply chain. For example, prior to their business operational phase, Map-on-Web should have followed the accountability lifecycle to be able to be accountable to any collaborating cloud provider and/or customer. Thus, the steps, which will be presented in the remaining of this section apply to the other cloud providers as well.

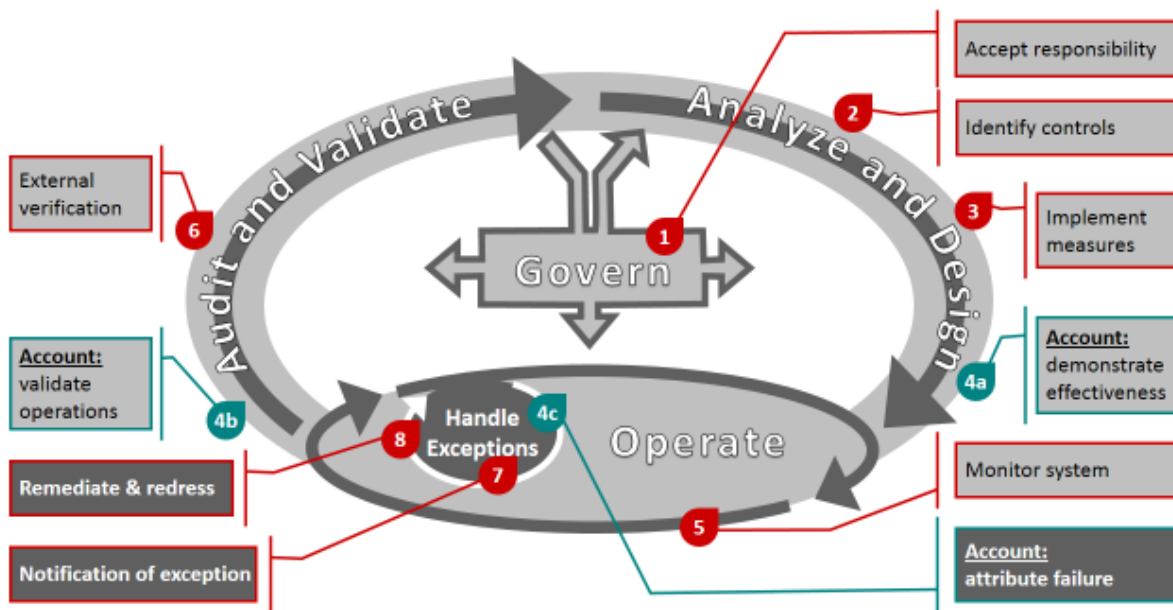


Figure 3: The functional elements of the Accountability Lifecycle

Having the above in mind, we start with the Analyse and Design Phase of the Lifecycle for CardioMon, which includes preventive accountability mechanisms and targets the processes that CardioMon should follow in order to select the cloud service chain to work with, given the security and privacy requirements that the Wearable Service should comply with. By accepting responsibility (functional element 1 in the Accountability Lifecycle), CardioMon has analysed the functional, security and privacy requirements of the Wearable service, taking into consideration the legal constraints for the implementation of an electronic service, involving processing of personal data. The requirements arise from the functionalities shown in Table 1, the type of data need to be collected, processed and stored, as depicted in Table 2, and the obligations that the specific provider has to accept in order to operate the cloud-based service, involving this data, in compliance with the data protection regulations.

Given these, CardioMon moves to the next functional element 2 of the Accountability Lifecycle, in which the responsible organisational staff (the Privacy Officer) need to find a cloud infrastructure provider fulfilling a given set of security and privacy requirements. This is shown in Figure 4, in which we present the interactions between the cloud and data protection roles for the accomplishment of the preventive accountability mechanisms for this use case. Addressing the 2<sup>nd</sup> functional element of the lifecycle, CardioMon decides to collaborate with DataSpacer and further investigate the necessary controls that should be implemented by CardioMon in the Wearable Service or supported by DataSpacer in the cloud environment setup to address the given privacy and security requirements. Thus, CardioMon performs a risk and data protection assessment for that data that will be processed in a cloud. The analysis of this assessment will guide CardioMon on whether and how to proceed with the development of the relevant cloud service. Figure 4 shows that this step is, also, adopted by the Wearable Co at a later stage to finally decide that CardioMon is the appropriate cloud provider to operate the Wearable Service on behalf of this cloud customer.

The proper implementation of the accountability measures (functional element 3 of the Accountability Lifecycle) implies that the Privacy Officer of CardioMon is responsible for defining the specific conditions, under which the implementation of the business level operations of Table 1, involving the data being listed in Table 2, can happen in an accountable manner. At this stage, the definition of the accountability policies refers to the default way that the CardioMon operational service will process the selected set of data being collected from all their cloud customers. When coming to the Wearable Co instance, a separate agreement between CardioMon and Wearable Co may apply (see Figure 4), which overrides the default one published by CardioMon and instantiates the defined accountability policies for the case of the Wearable Co operational cloud service (the instance of the Wearable Service). In both cases, the implementation of the accountability measures is concluded with the enforcement of the policies on the CardioMon side and the IT Director of CardioMon is ultimately responsible for the correct enforcement of these policies.



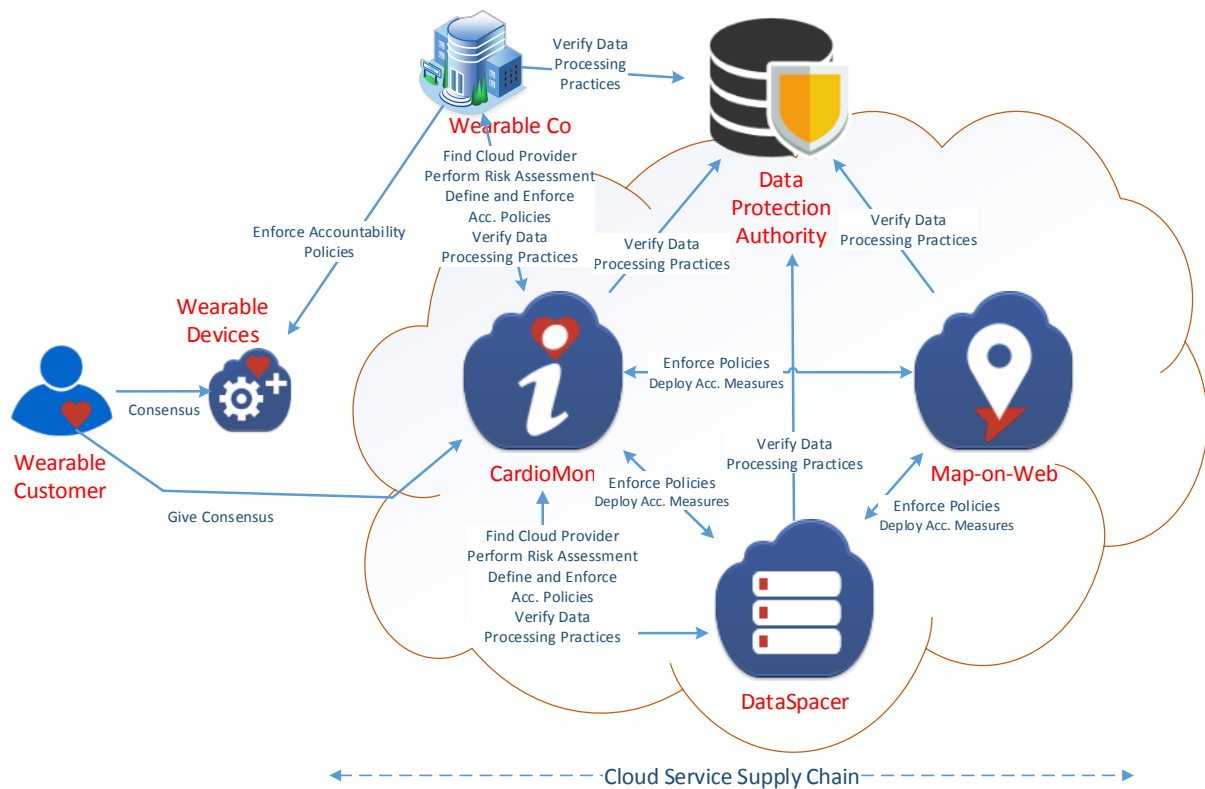


Figure 4: The perspective of the Wearable Use Case for the implementation of preventive accountability mechanisms

The perspective of the Analyse and Design Phase ends up with the deployment of the accountability measures, implemented in the previous steps, including the configuration of the monitoring, detection and auditing mechanism and the validation of these deployed mechanisms to the whole cloud service supply chain (as part of the implementation of preventive mechanisms shown in Figure 4). At this point, CardioMon collects the necessary account from the cloud service supply chain regarding the way that accountability is effectively deployed in this chain, through specific processes and tools. Moreover, CardioMon needs to verify that adequate data processing practices are in place by all cloud providers to support the operation of the target cloud service. CardioMon is, then, accountable to the Wearable Co for the proper accomplishment of this functional element 4 (a and b) of the lifecycle (being implemented by the IT department of CardioMon) by delivering to the CEO of Wearable Co the respective evidence of account, both by demonstrating the effectiveness of the deployed measures to support the obligations of CardioMon (and the subsequent cloud providers in the supply chain), arising from the regulations, the respective obligations (see Section 8.2) and identified privacy and security requirements, and showcasing the results of the validation of the data processing practices.

Upon completion of the Analyse and Design Phase, CardioMon is ready to operate its cloud service and, consequently, offer an instance of it to the Wearable Co. At this Operate Phase, the runtime monitoring of the Wearable Service is used to log user level actions (i.e. submit personal data for storage, request access to personal data previously collected, etc.), in order to gather evidence about the adopted data processing practices and use this evidence to prove verification of these practices to the collaborating cloud providers and customers for auditing purposes. As such, Figure 5 demonstrates the detective accountability mechanisms of the Wearable use case, which are partially implemented in this Operate Phase. In this phase, CardioMon, Map-on-Web and DataSpacer perform specific data protection related tasks to serve the application layer functions of the Wearable customers (which can be summarised as: providing personal data, through either their devices or the Web interface of the Wearable service, and accessing these data on a case-by-case basis). These providers exploit the deployed accountability measures to gather evidence (functional element 5 of the Accountability Lifecycle) about the compliance with data stewardship policies. The process of gathering evidence is materialised by the collection of various types of logs from the cloud environment. Depending on their cloud service deployment model, CardioMon, Map-on-Web and DataSpacer may use different tools to

generate logs from their inherent behaviour against the established accountability measures (such as the accountability policies) and collect logs from the interaction with the cloud environment.

These logs are, further, processed to build evidence records, which are exploited by the cloud providers to verify their data processing practices at runtime. These records are eventually used to detect incidents and anomalies reflecting potential policy violations and data breaches by developing the appropriate account for the attribution of failures (see functional element 4c of the Accountability Lifecycle).

The incident detection process is realised in the whole cloud service supply chain of the wearable use case. Each cloud provider is responsible for detecting incidents happening in their regime of responsibility or receiving requests and complaints about potential violation of the agreements. We emphasise different types of incidents, which may refer to various interactions and data protection control points spread across the Wearable service. The following Table 4 summarises the incidents, which are considered in the specification of this use case.

*Table 4: The incident types considered in the specification of the Wearable Use Case*

| No | Incident Type                        | Description of the incident   |
|----|--------------------------------------|---|
| 1  | Unauthorised Data Access             | The Wearable Co employee browses the list of registered wearable customers and requests to access the complete record of the personal information of a customer, which is not allowed by the specified policy. CardioMon raises a data access exception.  |
| 2  | Inadequate Data Retention / Deletion | The agreed accountability policy between CardioMon and the Wearable Co defines that the personal data collected from the customer's device must be deleted if being older than 6 months. However, a backup of the CardioMon store is left.  |
| 3  | Unauthorised Data Location           | The Wearable Co has agreed with CardioMon that only data centres in Europe are used for storing the personal data of the customers. A sudden hardware failure in DataSpacer results in the CardioMon store being moved to a third country location.   |
| 4  | Encryption vulnerability             | The Map-on-Web uses encrypted communication with CardioMon to access the personal information of the customers collected from their devices in order to generate the statistics per geographical area. However, at a specific period of time this communication turns to be unencrypted.        |
| 5  | Right to know vs. Need to know       | The Wearable Co employee performs too many requests to access the list of wearable customers and get their profile data. Although being an authorized party, the employee invokes the relevant service too many times, indicating an abuse of its right, hence a (probable) security violation. |
| 6  | Service unavailability               | The Wearable Customer requests the visualisation of statistical information, but the communication between CardioMon and Map-on-Web is broken.  |

At any time of the operational phase of the Wearable Service, the Audit and Validate Phase can run in parallel to the Operate Phase (and the other phases of the lifecycle), enabling cloud providers being accountable to the other collaborating providers, the Wearable Co and the Data Protection Authorities for verifying the declared data processing practices and demonstrating their compliance to the legal framework and their organisational policies (functional element 6 of the Accountability Lifecycle). This is achieved by allowing these actors access the auditing process of the cloud providers and generate audit reports, which entail the evidence-based verification of the data processing practices for specific accountability policy-based tasks.

Additionally, CardioMon must be able to showcase their data processing practices to the Wearable Co. Finally, the wearable customers may take control over the disclosure of their wellbeing data in the cloud

by tracking the data processing practices of CardioMon, and the subsequent practices of their third parties, such as Map-on-Web and DataSpacer.

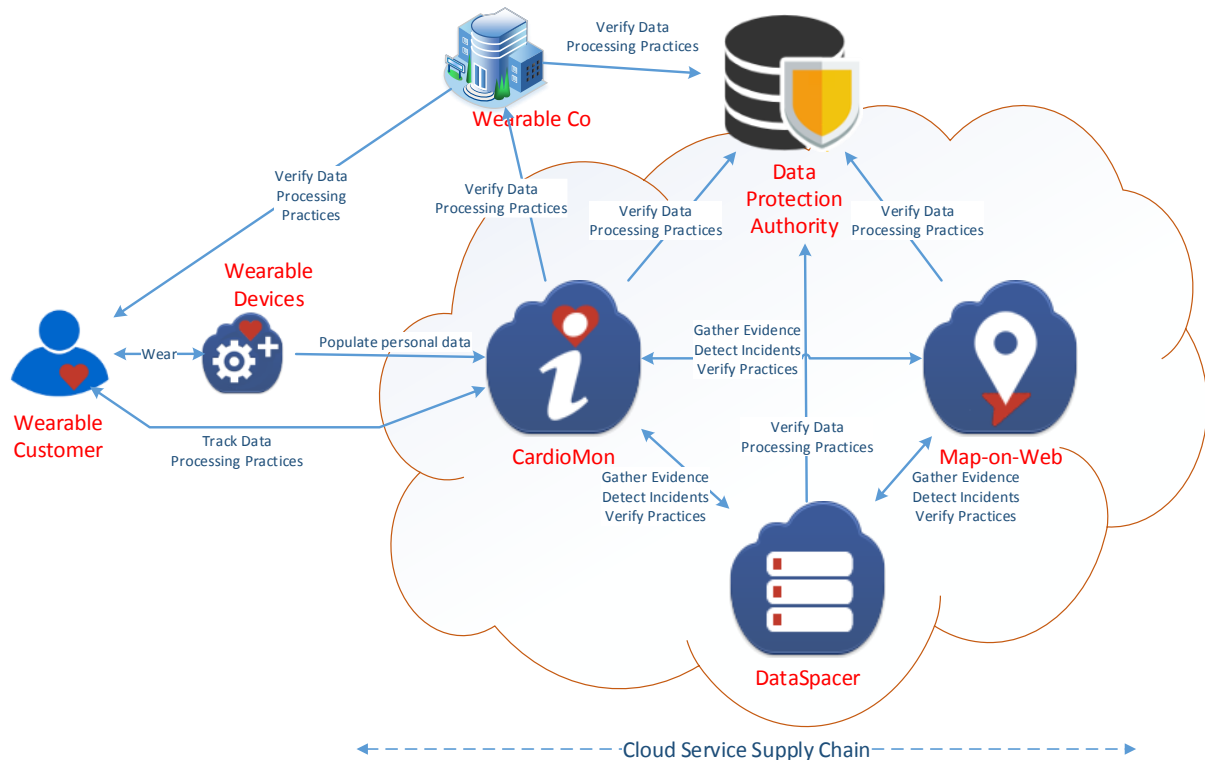


Figure 5: The perspective of the Wearable Use Case for the implementation of the detective accountability mechanisms

It has to be clarified that the verification of the data processing practices may refer to both internal and external audits. For example, the IT Director of CardioMon may require an internal audit on the supported data processing practices for the operation of the Wearable Service, while the CEO of the Wearable Co is subject to performing frequent external audits on CardioMon to verify their compliance to the agreed policies.

Moving to the Handle Exceptions Phase of the Accountability Lifecycle, the incidents detected in the various points of the cloud service supply chain (as shown in Figure 5) have to be communicated to the relevant stakeholders, according to the obligations arising from the legal framework and the specifications of the accountability policies. Figure 6 shows the implementation of the corresponding corrective mechanisms for the various actors in the wearable use case. As shown there, the parties responsible for the detection of incidents are accountable to their collaborating actors (accountees) for further implementing the respective remediation actions, ranging from simple notification reports on the type of detected incident (as per functional element 7 of the Accountability Lifecycle) to the actual redress and activation of controls (see functional element 8 of the Accountability Lifecycle) so that the cloud service provision returns to a normal behaviour.

As shown in Figure 6, at any time of this phase, the cloud providers involved in the Wearable use case have to adopt the functional elements of the Audit and Validate Phase. In that respect, the providers of accountability (accountors) can effectively demonstrate their compliance with the accountability policies, even in the case of an incident detection, while the cloud providers and customers receiving accountability assurance (accountees) can, at any time, request verification of their providers' data processing practices by receiving relevant audit reports.<sup>1</sup>

The detailed instantiation of the accountability framework for this prototype of the Wearable use case is performed in Section 4, based on the integration work described in Section 3.

<sup>1</sup> For a detailed analysis of the concepts on accountor and accountee, please refer to [1].

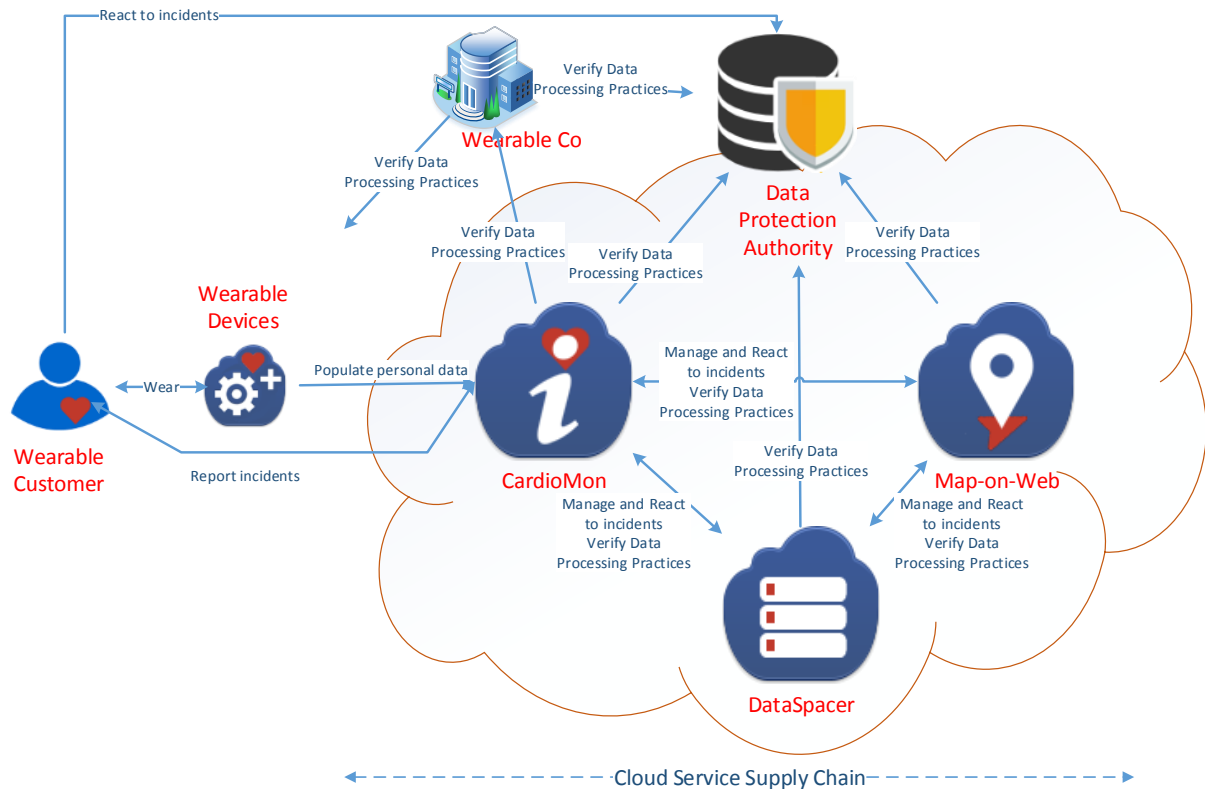


Figure 6: The perspective of the Wearable Use Case for the implementation of the corrective accountability mechanisms

### 3 Integration of the A4Cloud Components

#### 3.1 Instantiation of the Cloud Accountability Reference Architecture

This section presents the instantiation of the Cloud Accountability Reference Architecture (CARA), as it has been described in WP:42 and Deliverable D42.3 [4]. More specifically, we focus on how CARA is instantiated to explain the implementation of accountability across the wearable use case actors. In that respect, it presents the adoption of the accountability support services and the respective accountability artefacts from each actor of Table 3 and elaborates on the perspectives of the (preventive, detective and corrective) phases of the accountability mechanisms, explaining the use of the relevant A4Cloud tools.

For this version of the A4Cloud prototype, we focus on the tools that present a certain maturity level, with respect to their current capability to interface with other A4Cloud tools and the components of the Wearable Service, as a cloud-based application. Thus, currently, we can only use and demonstrate the following accountability support services, artefacts and A4Cloud tools:

- **Policy Definition and Compliance:** this service enables the cloud providers and customers to define and configure *Accountability Policies*, which are based on the functional, security and privacy requirements of these actors and the development of policy terms in accordance to their legal, normative or contractual *Obligations*. Contractual Obligations are used in this service to allow cloud providers specify their *Capabilities*, in terms of their cloud service offerings, which take the form of machine-readable contracts. Currently, the policy definition and compliance accountability support service is realised through the use of:
  - *COAT* for the selection of a compliant cloud service provider, based on its Capabilities.
  - *DPIAT* for the impact assessment regarding the use of a specific cloud service provider to process personal data. Impact assessment is based on the defined organisational and business

operations, exhibiting certain functional, security and privacy requirements, and the resulting Obligations.

- The machine-readable specification of the accountability policies, in the form of A-PPL, entailing the personal data to be handled by the providers and the access and usage controls over this data.

The policy definition and compliance accountability support service is based on a human readable representation of the privacy policies, which is translated to A-PPL, as defined in D:43.2 [5]. The presentation of the translation of human readable privacy policy to A-PPL is left for the final prototype.

- *Policy enforcement*: this service involves the execution of the data processing practices, in accordance to the policies defined in the previous step. The policy enforcement part engages the use of *A-PPLE* as the enforcement engine to allow data processing operations.
- *Collection & management of evidence*: this service is realised through the use of the following A4Cloud tools:
  - *A-PPLE*, which generates *logs* with respect to actual decisions made in the policy enforcement part.
  - *DTMT*, which monitors the cloud environment networking part and generates *logs* with respect to data transfers identified in it.
  - *AAS*, which monitors the various layers in protocol stack of the cloud service delivery models (SaaS, PaaS, IaaS, etc.) and collects *logs* that may relate to potential security breaches or policy violations.

During this accountability support service, the machine-generated logs collected by the above mentioned A4Cloud tools are used to compile *Evidence Records* about the operation of the Wearable Service by the involved cloud providers. This service also refers to the management of logs within their full lifecycle, according to specific integrity, confidentiality and access control requirements. At this stage of development, the evidence can only be built on the records produced by *AAS*.

This evidence is, then, exploited to support the demonstration of compliance to established and agreed data processing practices through the execution of (both internal and external) audits, using the *AAS UI* and the generation of *Audit Reports*, including evidence records and related objects such as related logs and policies.

Both the compilation of *Evidence Records* and the support for internal and external audits, through the relevant *Audit Reports* constitute the basis for the provision of the account, in order for the actors in this wearable use case to be accountable for their operations to their collaborating actors from Table 3. This will be, further, explained in Section 4.

- *Notification*: this service is partially supported in the first A4Cloud prototype by enabling the tools of the previous accountability support service (namely *A-PPLE*, *DTMT* and *AAS*) raising incidents about policy violations and security breaches. The incidents are communicated in the form of *Notification Reports*, enumerating the types of the detected incidents and other information specific to these incidents.

The *Notification* accountability support service will be completed in the final A4Cloud prototype and will be linked to the *Remediation* service. Furthermore, the Data Subject Enablement service, which is realised mainly by the use of *DT*, has not yet been integrated with the policy enforcement service and, thus, it has been excluded from this first prototype.

Following the above description, the first A4Cloud prototype instantiates the toolkit, by focusing on the support of the preventive and detective accountability mechanisms, along with the execution of the functionalities of the Wearable Service, as they are presented in Table 1. In that respect, the actors involved in the wearable use case exploit the A4Cloud tools as depicted in Table 5.

It is clarified that the whole timeline of the Wearable Service operation (starting from the development of DataSpacer, the operation of Map-on-Web and CardioMon and the implementation and operation of the cloud-based wearable use case on behalf of the Wearable Co) involves more accountability support

services and tools to be consumed by the wearable service actors. However, for the sake of this deliverable, we focus on the interactions described in this Table 5.

*Table 5: The first instantiation of the A4Cloud Cloud Accountability Reference Architecture for the wearable use case<sup>2</sup>*

| Wearable Service Actor | A4Cloud Tool   | Addressing Accountability Support Service              | Involving Accountability Artefact   |
|------------------------|--|--|---|
| Wearable Customer      | No tool support, but realised through the Wearable Service | Policy Enforcement (indirectly through giving consent) | Accountability Policies   |
| Wearable Co            | COAT   | Policy Definition and Compliance                       | <ul style="list-style-type: none"> <li>Capabilities of cloud providers</li> <li>Obligations</li> </ul>                    |
|                        | DPIAT  |  | <ul style="list-style-type: none"> <li>Capabilities of cloud providers</li> <li>Obligations</li> </ul>                    |
|                        | <i>Any text editor to manually edit A-PPL policies</i>     |  | Accountability Policies   |
| CardioMon              | COAT   | Policy Definition and Compliance                       | <ul style="list-style-type: none"> <li>Capabilities of cloud providers</li> <li>Obligations</li> </ul>                    |
|                        | DPIAT  |  | <ul style="list-style-type: none"> <li>Capabilities of cloud providers</li> <li>Obligations</li> </ul>                    |
|                        | <i>Manually created A-PPL</i>                              |  | Accountability Policies   |
|                        | A-PPLE   | Policy Enforcement                                     | Accountability Policies   |
|                        | A-PPLE   | Collection & management of evidence                    | Machine-generated logs  |
|                        | AAS  |  | <ul style="list-style-type: none"> <li>Machine-generated logs</li> <li>Evidence Records</li> <li>Audit Reports</li> </ul> |
|                        | A-PPLE   |  | Notification Reports  |
|                        | AAS  | Notification   |   |
| Map-on-Web             | <i>Manually created A-PPL</i>                              | Policy Definition and Compliance                       | Accountability Policies   |
|                        | A-PPLE   | Policy Enforcement                                     | Accountability Policies   |
|                        | A-PPLE   | Collection & management of evidence                    | Machine-generated logs  |
|                        | AAS  |  | <ul style="list-style-type: none"> <li>Machine-generated logs</li> <li>Evidence Records</li> <li>Audit Reports</li> </ul> |

<sup>2</sup> In the Collection & management of evidence accountability support service, the A4Cloud tools integrate TL.



| Wearable Service Actor | A4Cloud Tool                  | Addressing Accountability Support Service | Involving Accountability Artefact   |
|------------------------|-------------------------------|---|---|
|                        | A-PPLE                        | Notification                              | Notification Reports  |
|                        | AAS                           |   |   |
| DataSpacer             | <i>Manually created A-PPL</i> | Policy Definition and Compliance          | Accountability Policies   |
|                        | A-PPLE                        | Policy Enforcement                        | Accountability Policies   |
|                        | DTMT                          | Collection & management of evidence       | Machine-generated logs  |
|                        | AAS                           |   | <ul style="list-style-type: none"> <li>Machine-generated logs</li> <li>Evidence Records</li> <li>Audit Reports</li> </ul> |
|                        | A-PPLE                        | Notification                              | Notification Reports  |
|                        | AAS                           |   |   |

The actual use of the tools and the production of the accountability artefacts in the context of the accountability support services for the wearable use case will be presented in Section 4.

### 3.2 Physical Deployment of the A4Cloud First Prototype

The first prototype of the instantiated A4Cloud toolkit for the wearable use case has been deployed, following the steps provided in this section. This step-by-step analysis of the physical deployment is useful to understand the required deployment procedures, during the different phases of the accountability lifecycle for each provider. Although the physical deployment of the A4Cloud instantiation for the wearable use case prototype may include more components in the end, for the time being and for this section, we only focus on the use of DTMT, AAS and A-PPLE. It must be noted that the A4Cloud tools for the policy definition and compliance service (namely COAT, DPIAT and AccLab), are not depicted in this section, since they are used only once and as offline tools, during the analyse and Design Phase. On top of that they are manually configured to operate for the wearable use case, as it will be explained in Section 4.

DataSpacer is the IaaS provider, which deploys the cloud infrastructure. The physical deployment consists of an OpenStack [6] installation and for the project purposes it is being hosted at ATC premises. This installation uses the ninth release of OpenStack, which is called Icehouse [7]. The installation has been based on the three-node OpenStack architecture configuration [8], in which we have set up a Controller Node, a Network Node and two Compute Nodes. The Controller Node represents the heart of the OpenStack environment and controls the storage volumes for storing data in this infrastructure. DataSpacer manages the Controller Node and any other cloud service, through the OpenStack Dashboard. Any other service provider, like CardioMon and Map-on-Web use the OpenStack Dashboard with their own tenant account to manage the cloud infrastructure resources allocated to their VMs. The Network Node handles all the interconnection of the various Virtual Machines within the OpenStack installation environment and with the outside world.

Additionally, DataSpacer configures two Compute Nodes, each one simulating a distinct geographic zone, and each one capable of hosting tenant virtual machines (VMs) or instances. In the DataSpacer case, Compute Node 1 embodies the data centres physically located in the territory of Europe, while Compute Node 2 embodies the data centres physically located in the territory of USA. Finally, a storage volume is provided by DataSpacer, which can be potentially attached to the VMs, either in Compute Node 1 or 2.

From an accountability perspective, the deployment of the A4Cloud tools in the DataSpacer area of responsibility 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 Admin of DataSpacer deploys the relevant A4Cloud tools, namely DTMT and AAS. This is shown in Figure 7.

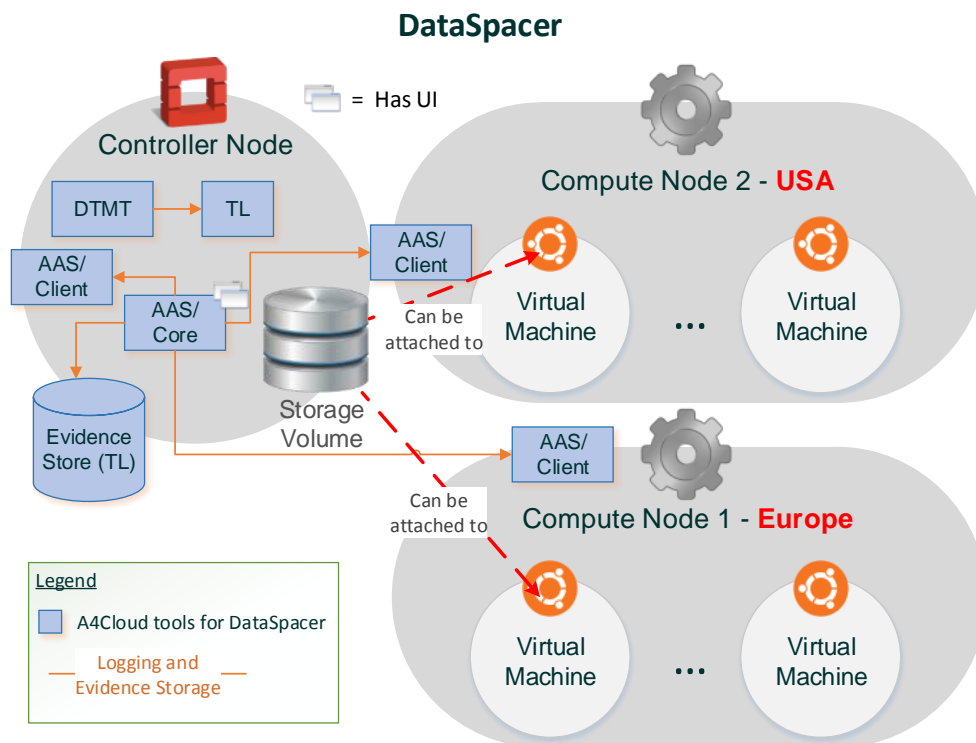


Figure 7: The deployment of the A4Cloud tools in DataSpacer

The Controller Node hosts DTMT to collect logs about data transfers happening within the DataSpacer environment, as they are captured on this node. DTMT embeds a TL instance, which is used to log any actions related to data transfers. Furthermore, the core version of AAS is deployed in the Controller Node to provide the processing of logs collected from the IaaS layers of DataSpacer. These logs are collected through the AAS clients, which are deployed in each Compute Node. DataSpacer maintains a central Evidence Store, operated by AAS Core, which uses a TL instance for secure and encrypted storage of the DataSpacer evidence records. The latter are invoked in case that an external or internal audit is requested through the UI of AAS Core.

Based on this infrastructure and deployment, DataSpacer allocates cloud resources to Map-on-Web and CardioMon to host their SaaS offerings and provide cloud services to their potential customers. In the wearable use case, we assume that both Map-on-Web and CardioMon select to use the data centres in Europe. So, DataSpacer allocates the requested resources from Compute Node 1 in the form of VMs. Both Virtual Machine 1 and Virtual Machine 2, which will eventually host the Map-on-Web and CardioMon respectively, are running a 64 bit Ubuntu Operating System version 14.04 [9].

Within each VM (1 and 2), the relevant SaaS cloud provider will have to deploy their own accountability tools. Of particular interest for this case is the deployment of the policy enforcement tool (A-PPLE) and AAS. Figure 8 shows how Map-on-Web complements the view presented in Figure 7, when this cloud provider enters into the picture and has to analyse personal data for any purpose. As it can be seen there, Map-on-Web deploys an instance of A-PPLE to enforce policy rules on the PII processed by the Map-on-Web service. Any action happening in A-PPLE is logged in the TL. The latter, then, enables a client of the AAS in this provider collecting these logs and transforms them to evidence records. Map-on-Web maintains its own evidence store for facilitating audits on the evidences gathered within the area of responsibility of Map-on-Web.



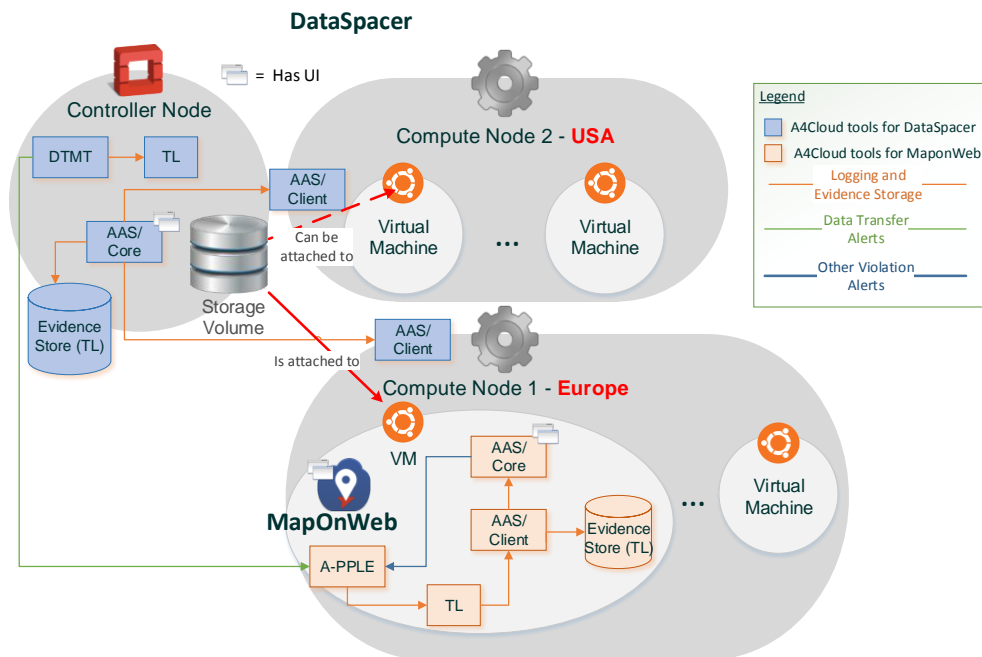


Figure 8: The deployment of the A4Cloud tools for the collaboration of DataSpacer with Map-on-Web

Following the same approach, CardioMon reserves its own cloud resources through a dedicated VM in Compute Node 1 of DataSpacer and deploys the respective A4Cloud tools. Figure 9 demonstrates the deployment of the cloud environment and the A4Cloud tools for the wearable use case. As it can be seen there, similarly to Map-on-Web, CardioMon creates its own instances of the A4Cloud tools. Within each VM, each cloud provider maintains its own log collection flow (captured with the orange highlighted arrows of Figure 9), using the following components:

- The TL instance embedded 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).
- The AAS client, which is used to collect the logs of the TL and transform them to evidence records, before they are maintained in the Evidence Store instance. The AAS client is, also, used to collect the logs from the cloud layers of VM 1 or 2 for Map-on-Web or CardioMon, respectively.
- Indirectly, the DTMT, which forwards any data transfer logs (maintained in the TL instance of DataSpacer) as a potential data transfer violation alert (green arrows in Figure 9) and this is, subsequently, logged by the TL instance of A-PPLE and the AAS client.

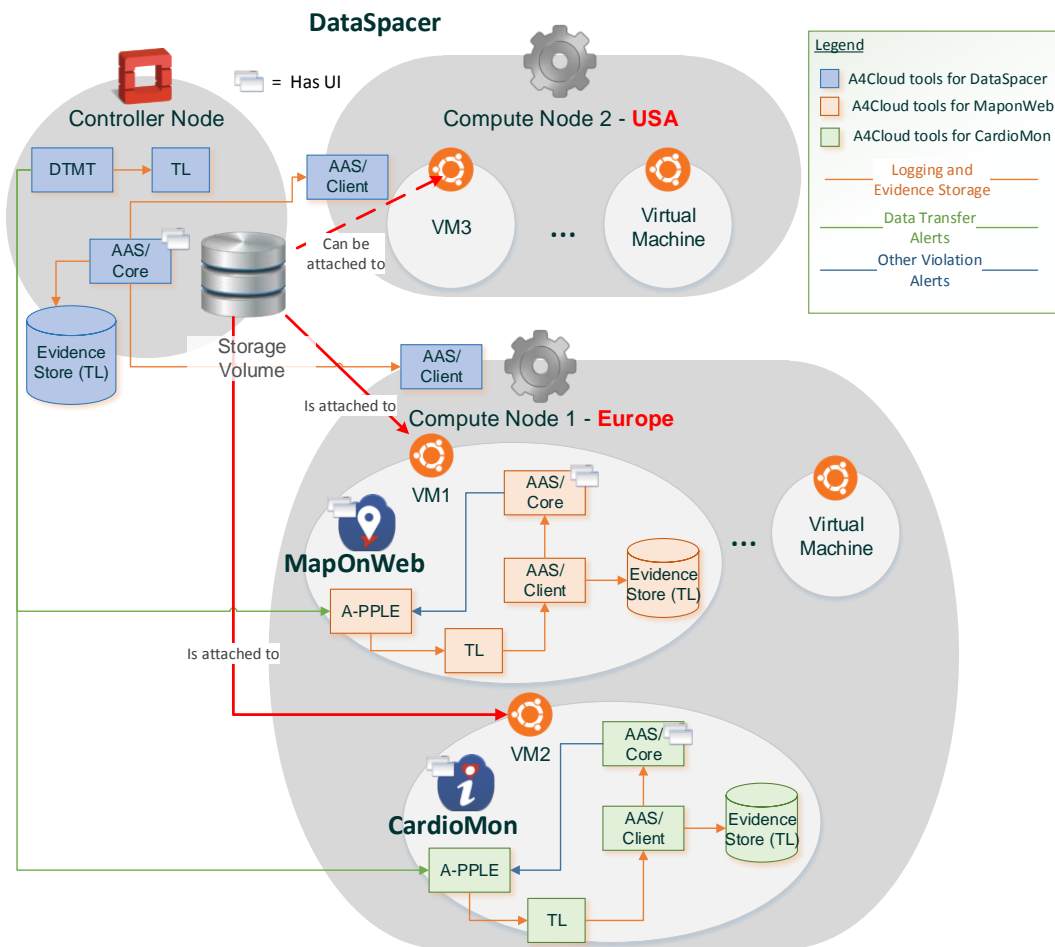


Figure 9: The physical deployment of the A4Cloud tools for the complete cloud service supply chain of the wearable use case

Apart from logging and evidence storage purposes, as mentioned above, Figure 9, also, shows the interactions between the tools in case of generating alerts for the purpose of potential violations. Thus, green arrows reflect the communication of DTMT with the configured A-PPLE instances in cases of data transfer incidents. An example is shown with the red arrows in Figure 9. As shown there, we assume that the storage volume provided by DataSpacer is, initially, allocated to VM1 and 2, both belonging to Compute Node 1 and physically located in Europe. Due to some reason, this storage volume, which can maintain the data created within the VM 1 and/or 2, is detached from Compute Node 1 and is attached to Compute Node 2, which physically located in USA. This can potentially raise a data transfer exception, in case that the accountability policy specifies that data collected and processed by CardioMon, for instance, should be maintained in Europe. In this respect, DTMT should log this transfer action on their own TL instance in DataSpacer and inform the A-PPLE instance of CardioMon, as reflected by the green arrow.

Another type of tool interactions arises from the incident types shown in Table 4. In that respect, some types of incidents (namely 2, 4, 5 and 6) are discovered by the AAS client of CardioMon, should be stored in the relevant instance of Evidence Store and be analysed by the respective AAS Core of CardioMon, which is responsible for raising an alert to the A-PPLE instance of CardioMon about the type of detected violation.

### 3.3 Guidelines for Use Case Developers

This section is dedicated to the developers that want to build their own use case, based on the accountability framework. We use as an example the steps we have followed (or need to follow) in order to set up the necessary environment and prepare the use case development for the wearable use case.

The example is provided in the form of guidelines for the potential use case developers. The presentation of this section is elaborated from the perspective of the accountability support services (see Table 5), which implement specific functional elements of the accountability lifecycle, as it was described in Figure 3.

It must be noted that this section facilitates architectural specifications for the potential use case developers and aims to go beyond the work done for the first prototype. In this sense, it extends the accountability support services presented in Section 3.1 and tries to cover the specifications of the whole Accountability Lifecycle.

### 3.3.1 Policy Definition and Compliance

In the policy definition and compliance service, the relevant cloud provider or customer SMEs use COAT in order to assess the Capabilities of the available cloud providers and select a cloud service (or service supply chain) to work with. This is the case of the Wearable Co, which is assisted in the selection of CardioMon for hosting and running the Wearable Service. As shown in Figure 10, the Wearable Co defines the business operations that need to be supported (such as the ones presented in Table 1) and lists the arising functional, security and privacy requirements in the form of Obligations. The latter involve the contractual bindings of the collaborating parties, the restrictions introduced by the legal framework for the support of the business operations and the ethical sense to support accountability in order to deliver these business operations in a secure and privacy enabled manner, through the cloud environment.

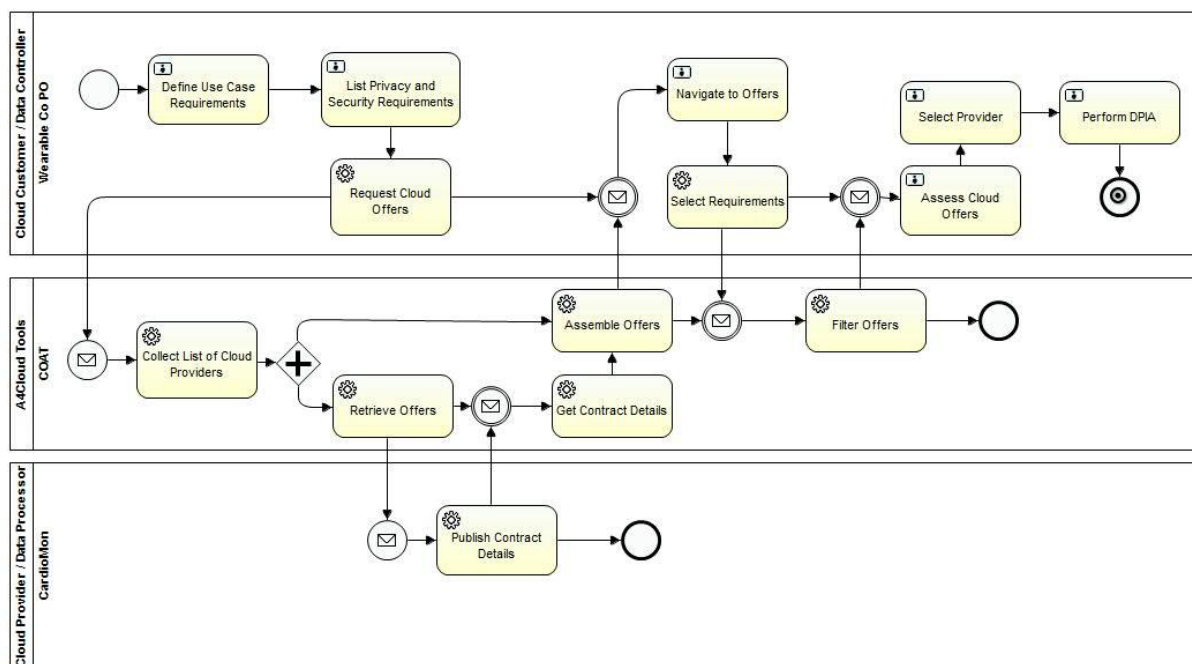


Figure 10: The process of the Wearable Co to use COAT in order to select CardioMon

Figure 10 reflects that the Privacy Officer of the Wearable Co uses COAT in order to match their requirements for the development of the Wearable Service with the Capabilities of CardioMon. By following COAT, the Privacy Officer of the Wearable Co can assess the capabilities of CardioMon and select this provider as the cloud operator of the Wearable Service. By settling down this decision, an additional step is executed. The Privacy Officer of the Wearable Co needs to assess the impact of selecting CardioMon for processing personal data collected from the Wearable Service in this cloud environment. This process, which is presented in Figure 11, involves the analysis of the implications of the data processing requirements for the specific business operations held in the selected cloud setting. By successfully completing this step, the respective policy editor has performed all the necessary compliance checks to start developing the accountability policies.

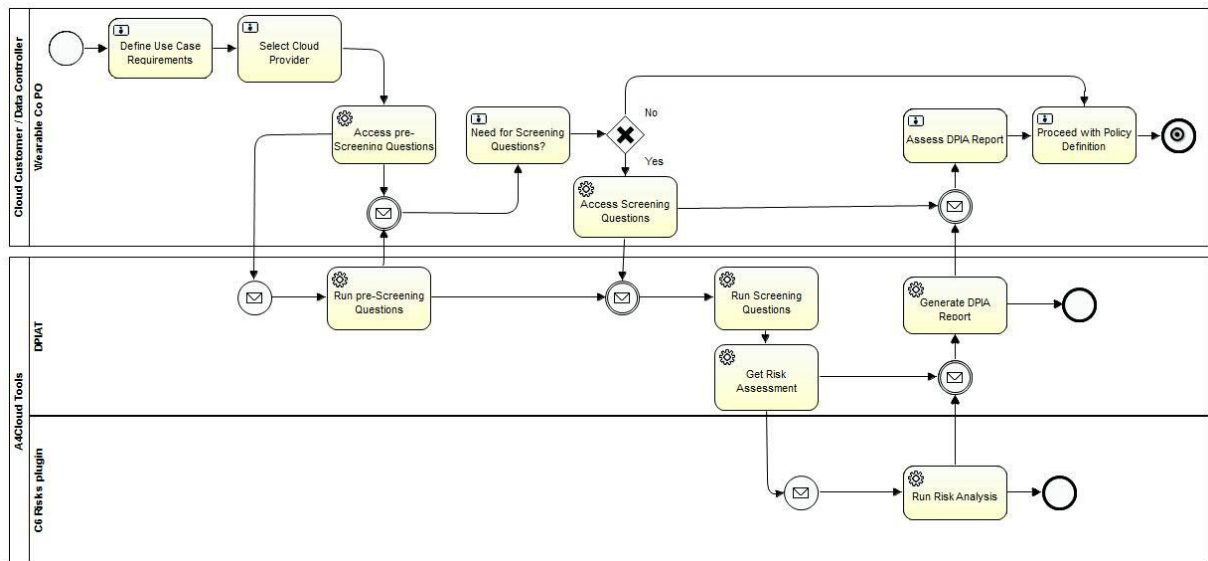


Figure 11: The process of the Wearable Co to use COAT in order to select CardioMon

The policy definition part starts with the specification of the privacy policy. This policy is derived by a Privacy Officer and takes the form of a legal document, which has to be enforced by an ICT tool (the A-PPL Engine in our case). We take as an example the case of CardioMon. The Privacy Officer of CardioMon elaborates on the CardioMon obligations and the business operations (functionalities) of the cloud service that has to provide. These will determine the rules of the lawyer readable privacy policy. In order for this policy to be enforced, along with the cloud service, the lawyer readable privacy policy will be translated to a machine readable accountability policy (in A-PPL format).

The process for delivering the machine readable accountability policy is presented in Figure 12. As shown there, the Privacy Officer of CardioMon can select two alternative flows. The first flow involves this actor to use a tool so that to express the lawyer readable privacy policy to the requirements of a Privacy Level Agreement (PLA) and the tool (PLAT<sup>3</sup>) to translate this PLA to an A-PPL accountability policy. As an alternative, the Privacy Officer can appoint a policy expert to translate the lawyer readable privacy policy to the intermediate AAL policy and, then, the expert uses AccLab to come up with the A-PPL and check the compliance of this policy with the defined data handling practices. In both cases, the outcome is a set of accountability policies in A-PPL format, which describe the policy targets (the PII) and the access and usage control rules, such as rules on data access, data retention and deletion and data transfer.

When this privacy policy is agreed with the Privacy Officer of the Wearable Co at a later stage, in order for the CardioMon cloud service to operate the Wearable Service, the rules and restrictions of this policy should be presented to the wearable customers in a user friendly manner, thus this policy to be human readable.

<sup>3</sup> PLAT will be introduced in the next version of the Accountability Reference Architecture (see work in WP42). The scope of this tool is to enable the semi-automatic translation of PLA statements to machine readable A-PPL rules.

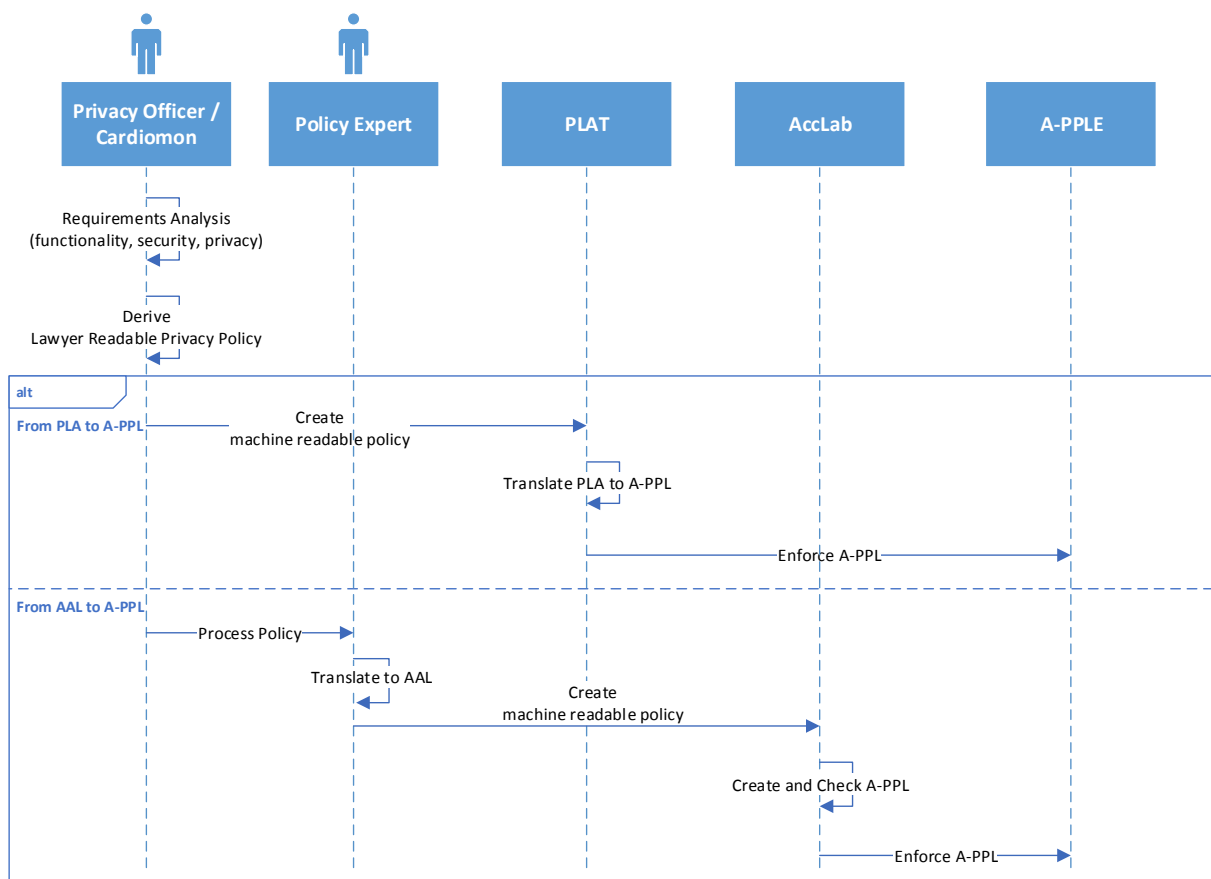


Figure 12: The alternative flows for the generation of the machine readable accountability policies

A step prior to the actual enforcement is the deployment of the relevant tools in the territories of each cloud provider. The deployment process for an instance of an A4Cloud tool does not differ among the cloud providers of the wearable use case, but it follows the same steps and it happens in different a timeline. As such and following the timeline realised from the storyboard of this use case (see Section 2.1), the deployment of the tools in the various cloud providers is evolved, as explained in the following lines.

#### Deployment of DataSpacer:

##### *Deployment of DTMT at the Controller Node of DataSpacer*

DataSpacer is running the cloud OS listed in Section 3.2 (three-node architecture of the Icehouse version of OpenStack) and needs to deploy an instance of DTMT on their Controller Node.

The IT Admin of DataSpacer should follow the instructions of [15] to deploy an instance of DTMT in the Controller Node of DataSpacer.

In order to test the proper deployment of DTMT to capture data transfers happening within DataSpacer, the IT Admin attaches a storage volume to Compute Node 1 and then detaches it from this node and attaches the volume to Compute Node 2 (this is reflected in Section 3.2 and Figure 9).

##### *Deployment of AAS to DataSpacer:*

The IT Admin of DataSpacer should follow the instructions in [16] to deploy an instance of AAS in the Controller Node of DataSpacer. As shown in Figure 9, DataSpacer configures two AAS client instances, which monitor the respective Compute Nodes 1 and 2 respectively to collect evidence about the processing of data along the cloud layers of DataSpacer.

#### Deployment of Map-on-Web:

The Map-on-Web service is installed in a VM created at DataSpacer for the exclusive use of this cloud SaaS provider. This VM is allocated a dual core CPU and 2 GB of RAM. The VM operates a 64 bit Ubuntu OS version 14.04 and runs Apache HTTP server 2.4 [10] and Apache Tomcat server 7 [11].

As shown in Figure 9, this VM hosts an instance of A-PPLE and an instance of AAS.

*Deployment of A-PPLE to Map-on-Web:*

The IT Admin of Map-on-Web deploys A-PPLE in the VM of Map-on-Web, based on the instructions provided in [5].

After completing the steps listed in the A-PPLE ReadMe file, A-PPLE is considered to have successfully been deployed in the VM of Map-on-Web. A final step involves the communication of the IT Admins of Map-on-Web and DataSpacer to configure DTMT of DataSpacer, so that it points to the A-PPLE instance of Map-on-Web, in case that a relevant policy rule about data transfers with reference to Map-on-Web happens.

*Deployment of AAS in Map-on-Web:*

The IT Admin of Map-on-Web should follow the instructions in [16] to deploy an instance of AAS in the VM of Map-on-Web.

As shown in Figure 9, Map-on-Web configures AAS client instance, which is used to monitor the actions happening on the potential log sources in this VM. Thus, AAS client is used to monitor and collect evidence about the processing of data along the cloud layers of Map-on-Web, as well as to monitor the actions logged from the A-PPLE of Map-on-Web and translate them to evidence records.

*Deployment of TL in Map-on-Web*

In order to facilitate both encrypted and secure log storage and communication, TL is deployed by the IT Admin of Map-on-Web<sup>4</sup>.

Deployment of CardioMon:

The CardioMon cloud operation for the Wearable Service is installed in a VM created at DataSpacer for the exclusive use of this cloud SaaS provider. As in the case of Map-on-Web, this VM is allocated a dual core CPU and 2 GB of RAM. The VM, again, operates a 64 bit Ubuntu OS version 14.04 and runs Apache HTTP server 2.4 and Apache Tomcat server 7. As shown in Figure 9, this VM hosts an instance of A-PPLE and an instance of AAS.

*Deployment of A-PPLE in CardioMon:*

The IT Admin of CardioMon follows the same instructions as the ones for Map-on-Web.

A final step involves the communication of the IT Admins of CardioMon and DataSpacer to configure DTMT of DataSpacer, so that it points to the A-PPLE instance of CardioMon, in case that a relevant policy rule about data transfers with reference to CardioMon happens.

*Deployment of AAS in CardioMon:*

The IT Admin of CardioMon follows the same instructions as the ones for Map-on-Web. As shown in Figure 9, CardioMon configures an AAS client instance, which is used to monitor the actions happening on the potential log sources in this VM. Thus, the AAS client is used i) to monitor and collect evidence about the processing of data along the cloud layers of CardioMon, and ii) to monitor the actions logged from the A-PPLE of CardioMon and translate them to evidence records.

*Deployment of TL in CardioMon*

In order to facilitate both encrypted and secure log storage and communication, the IT Admin of CardioMon deploys TL, as per the instructions followed by the IT Admin of Map-on-Web.

---

<sup>4</sup> In order to test the deployment of TL, the IT Admin of Map-on-Web uses a Secure Shell (SSH) client (like PuTTY [14]) to create three instances and run the indicating shells, namely sender.sh, recipient.sh and demo.sh. Running the latter, the IT Admin successfully sees the logs, giving the correct output in the first two parts.

### **3.3.2 Policy Enforcement**

During the policy enforcement accountability support service, the accountability policies are enforced in A-PPLE and the associated A4Cloud tools are configured, based on the policy rules. The enforcement is triggered by the CardioMon IT Administrator, who is responsible for the deployment of the necessary A4Cloud tools in the territory of CardioMon. As per Table 5 and Figure 9, these tools include A-PPLE and AAS, which embed TL for the secure and encrypted storage of logs. For this reason, the process that is depicted in Figure 13 is followed. In this figure, the IT Admin of CardioMon enforces the A-PPL accountability policy, as it was derived from the flow of Figure 12, into the A-PPLE instance of CardioMon. The rules of this policy have to be distributed to all the involved tools of CardioMon and the respective tools of both Map-on-Web and DataSpacer.



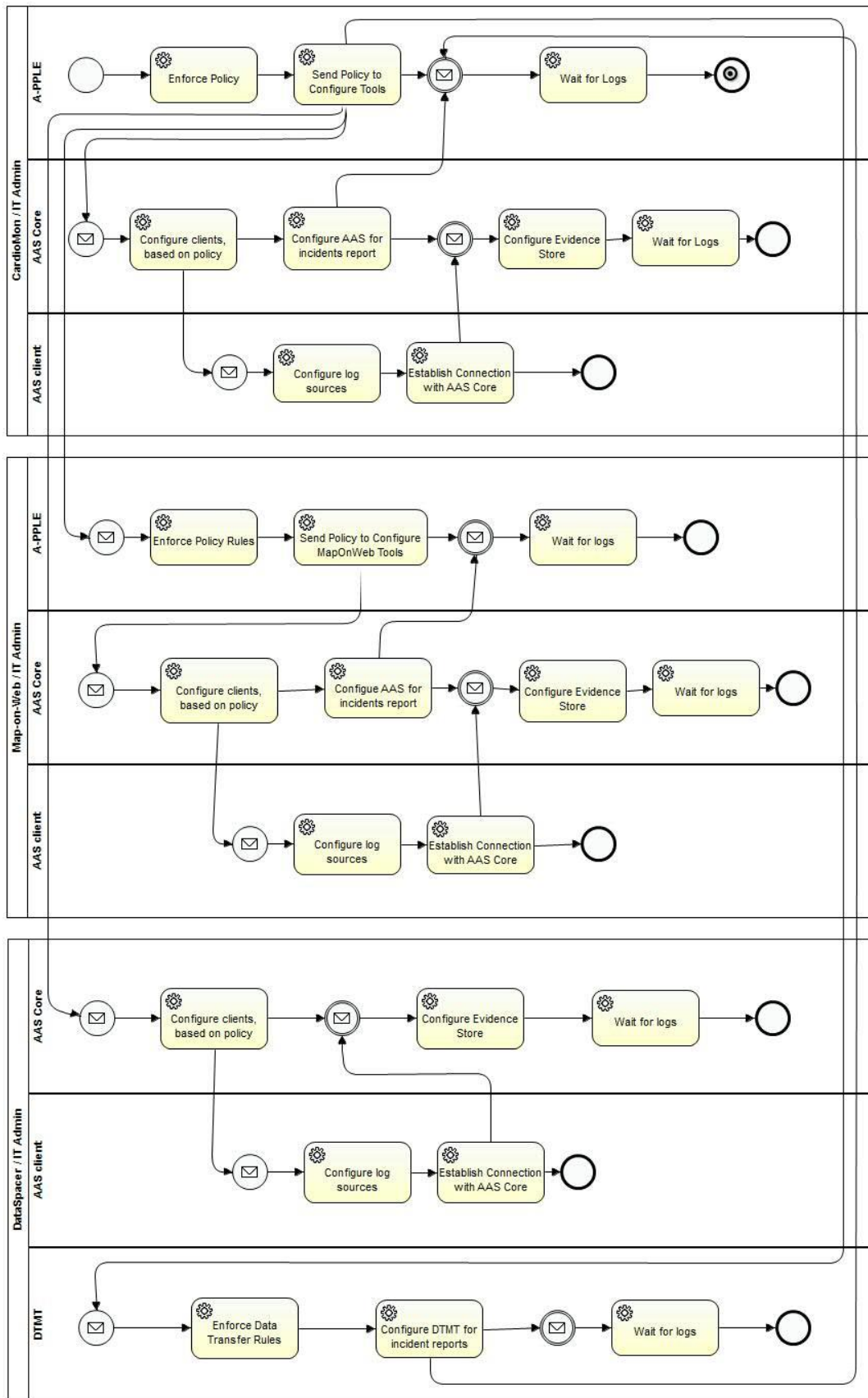


Figure 13: The process for the enforcement of the policy rules in the various actors of the wearable use case



### 3.3.3 Collection & management of evidence

During the collection and management of evidence accountability support service, the runtime operation of the business application is being monitored and the relevant business application functionalities are checked against the enforced policies.

In principle, and for the time being, we focus on three types of actions to be monitored from a data protection perspective, namely data access, data retention and data transfer. All the business application layer functionalities can be seen in these three data protection actions, which are analysed in the following to provide the view of the A4Cloud tools interactions, along with the connection to specific examples from the Wearable Service.

For the data access case, we consider the example of implementing F12 (see Table 1) about an employee of the Wearable Co browsing through the list of registered users and their profile. Figure 14 shows how the different A4Cloud tools interact with each other and with the application to determine on the employee access rights to the PII of the wearable customers.

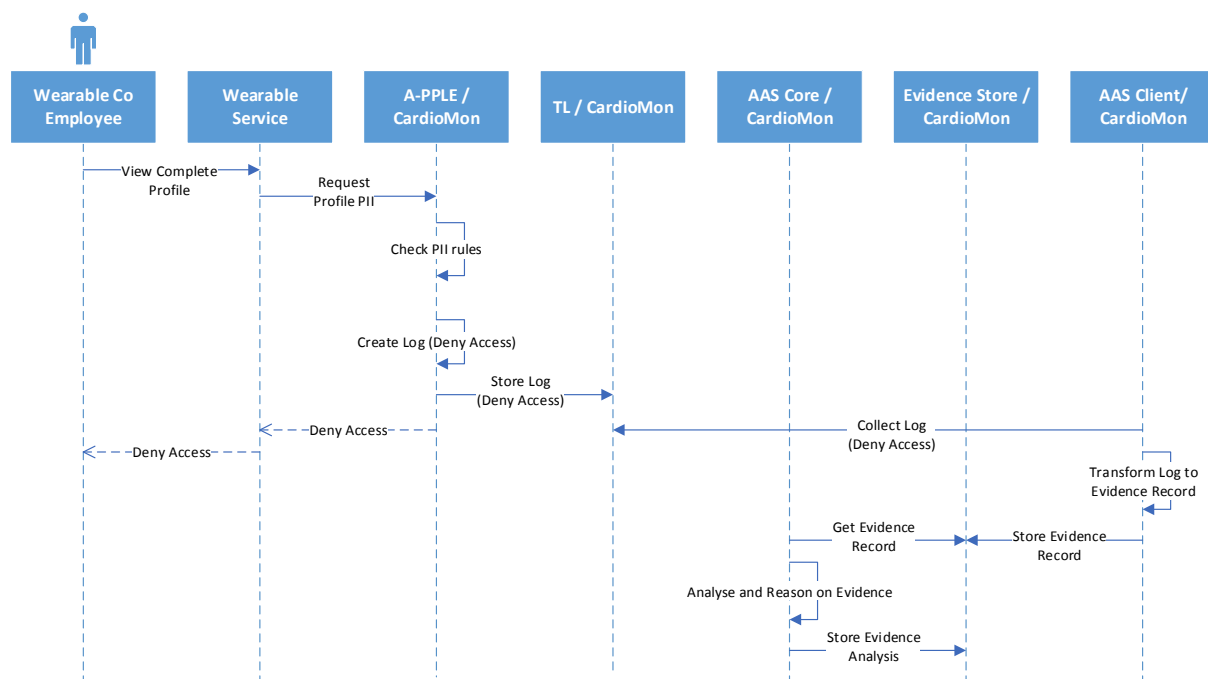


Figure 14: An example process for the collection and management of evidence in case of a data access incident

In the case of a data retention action, we consider the example that the PII store of the A-PPLE instance in CardioMon is backed up, through the CardioMon IT Administrator using their tenant account in the DataSpacer Dashboard. The action of creating a snapshot of the PII store of the A-PPLE instance in CardioMon is logged by the respective AAS client of CardioMon.

When a data retention rule is applied in the PII store of the A-PPLE instance of CardioMon, a specific dataset of personal data is deleted, but this action is not populated in the corresponding dataset of the snapshot. AAS Core instance of CardioMon analyses the evidence records created by AAS client (see Section 4.5 for more details) and raises an incident to A-PPLE to check for a potential violation of the accountability policies.

This example process is shown in Figure 15.

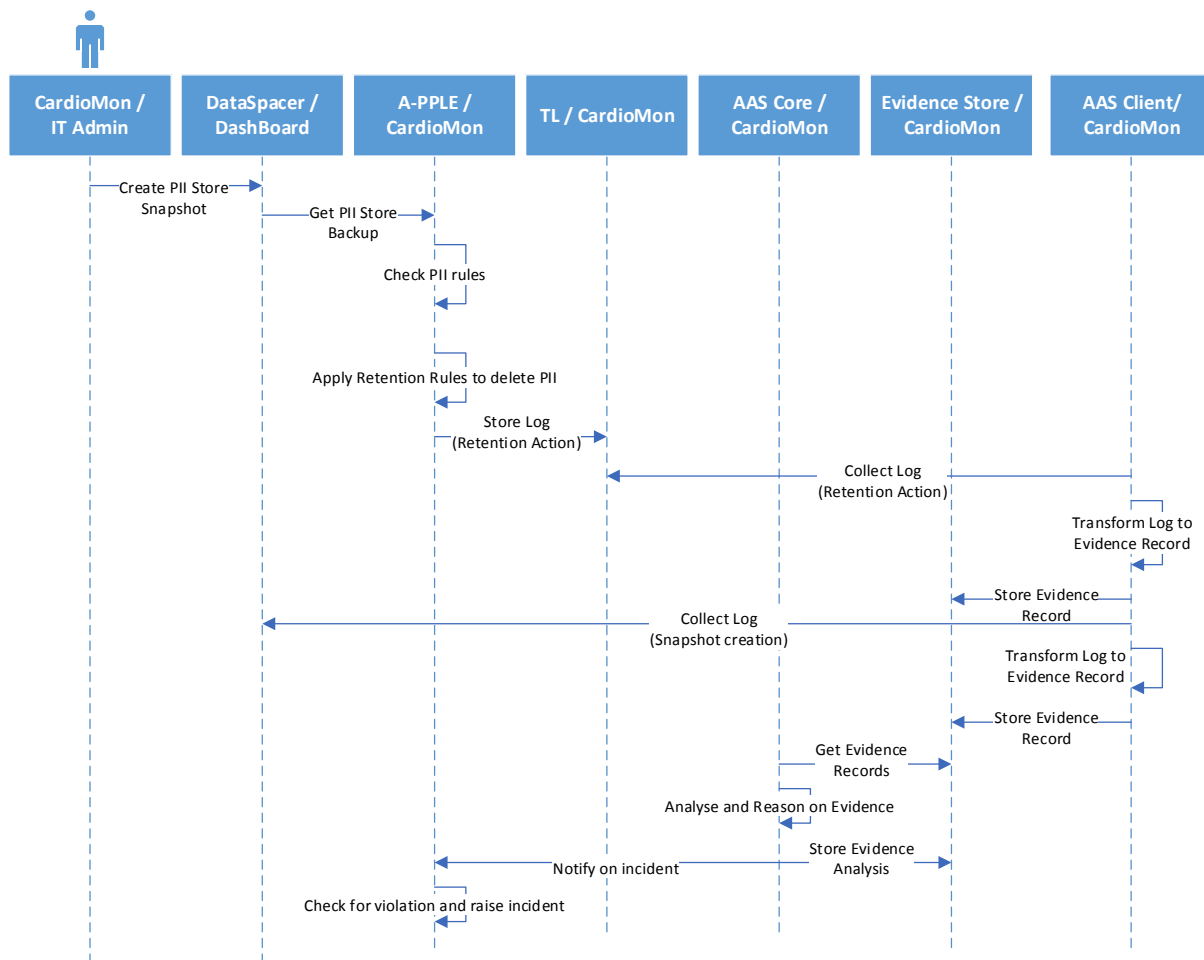


Figure 15: An example process for the collection and management of evidence in case of a data retention incident

A third case of evidence gathering relates to the example of a data transfer action. As shown in Figure 16, due to an emergency situation, the IT administrator of DataSpacer decides to detach the data volume attached to CardioMon (Compute Node 1 – Europe) and attach it to Compute Node 2 – USA. This is depicted in Figure 9 and has already been explained in Section 3.2.

This data move is detected by DTMT, which collects the appropriate logs and notifies the A-PPLE instance of CardioMon about this incident, which could be a potential violation. The evidence gathering process follows the same steps for any action happening within A-PPLE.

In all these cases, the AAS Core UI is used for internal and external audit by the various auditors, who can configure specific audit tasks and get the relevant audit reports. The latter are produced by analysing and combining the records included in the Evidence Store of each cloud provider.

In the first prototype, AAS only collects logs from the cloud environment and it cannot store evidence records produced from the analysis of the logs created by A-PPLE or DTMT.

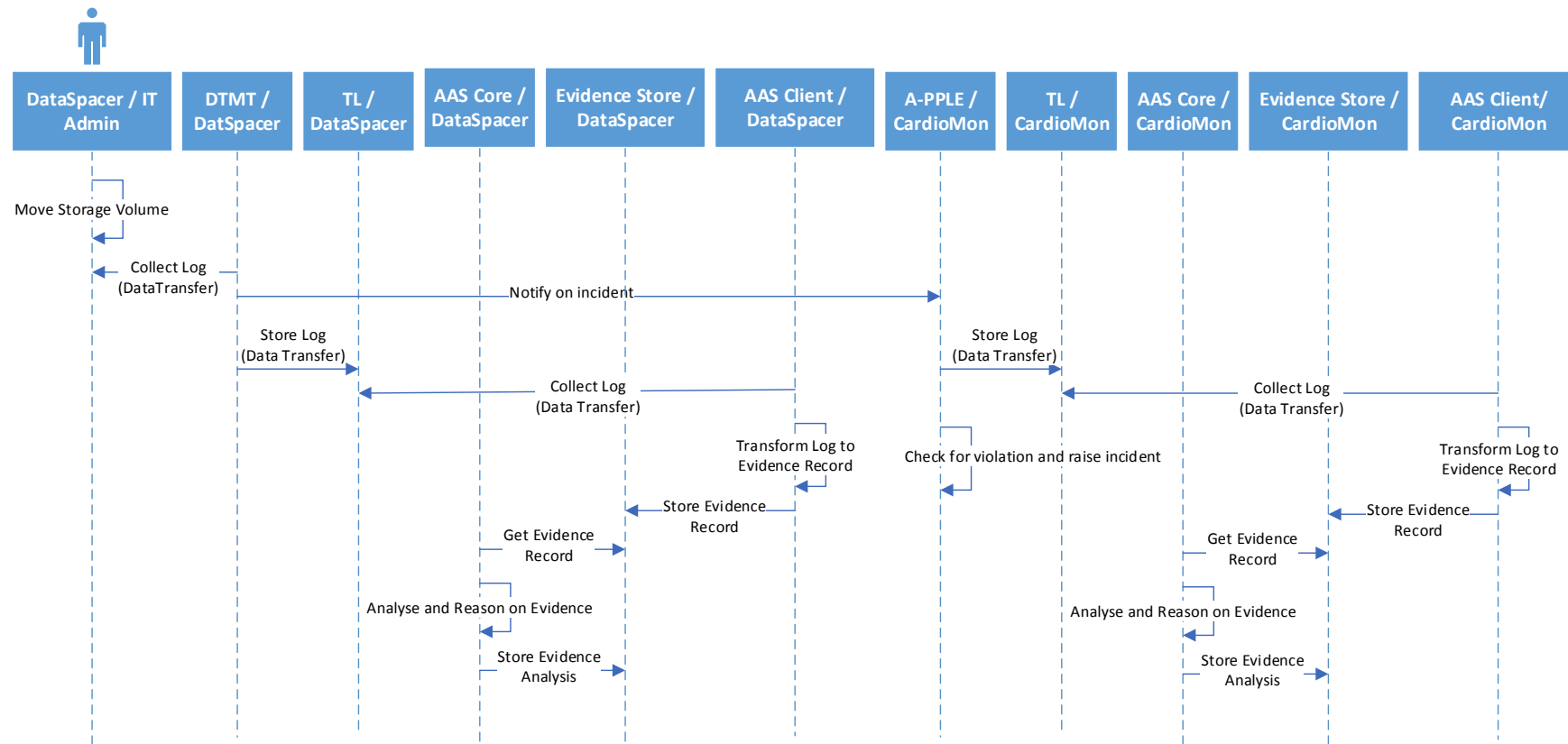


Figure 16: An example process for the collection and management of evidence in case of a data transfer incident

### 3.3.4 Data Subject Enablement

In the data subject enablement accountability support service, data subjects are provided a tool to take control over which of their personal data is maintained by various cloud providers and review whether the processing of these data is in accordance to one-to-one agreements with the respective data controller.

This service is mainly accomplished by DT and A-PPLE. For the case of the Wearable Service, DT should be configured to interoperate with the A-PPLE instance of CardioMon and for the specific wearable customer of reference. This is only achieved if DT is integrated with the Wearable Service, with the way that is depicted in Figure 18.

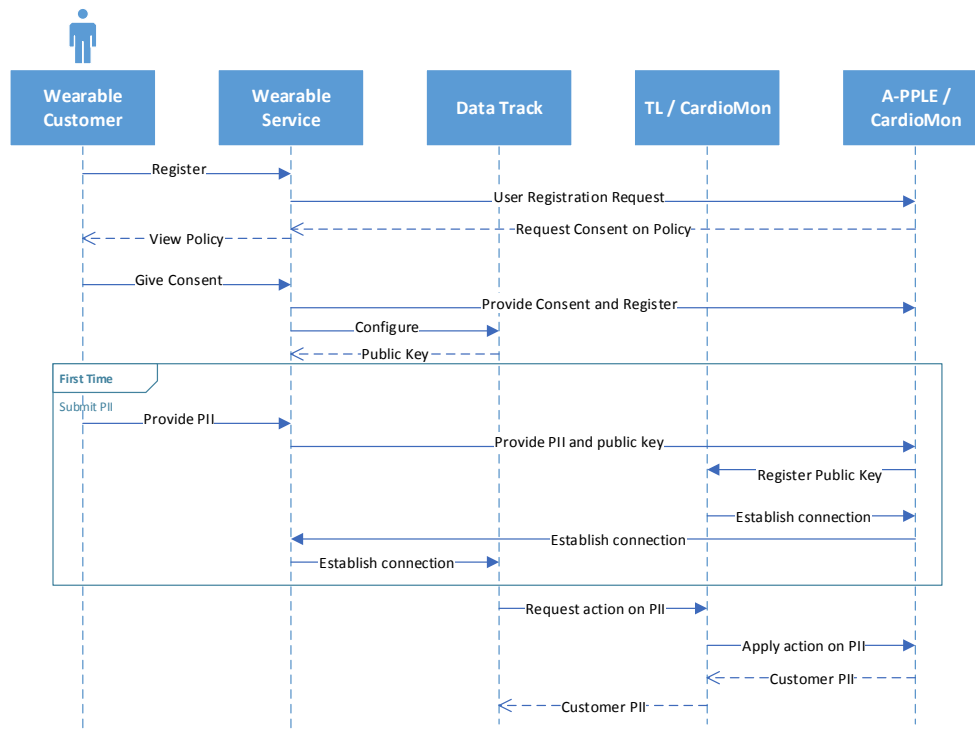


Figure 17: The implementation of the data subject enablement process

This accountability support service has not been implemented for this First Prototype.

### 3.3.5 Notification and Remediation

As shown in Section 3.3.3, the results of the detective phase and the evidence gathering part drive the detection of incidents, which should be managed by the respective A4Cloud tools in the corrective phase. The incidents that can be detected in the cloud environment are populated in the A-PPLE instance of the respective cloud provider, which is the responsible tool to generate policy violation alerts and activate the notification and remediation process.

The latter accountability support services are implemented with the involvement of IMT and RRT, which are the respective tools dealing with the corrective accountability mechanisms. As such, Figure 18 shows the process for the implementation of the notification accountability support service. As shown there, IMT refers to the cloud providers and data controllers, as the A4Cloud tool to enable management of the incidents received from A-PPLE. IMT is responsible to determine the level of notification (what to notify), the recipients of the notification action and the way to notify these recipients, according to the specification of the accountability policies.

This accountability support service has not been integrated in this First Prototype.

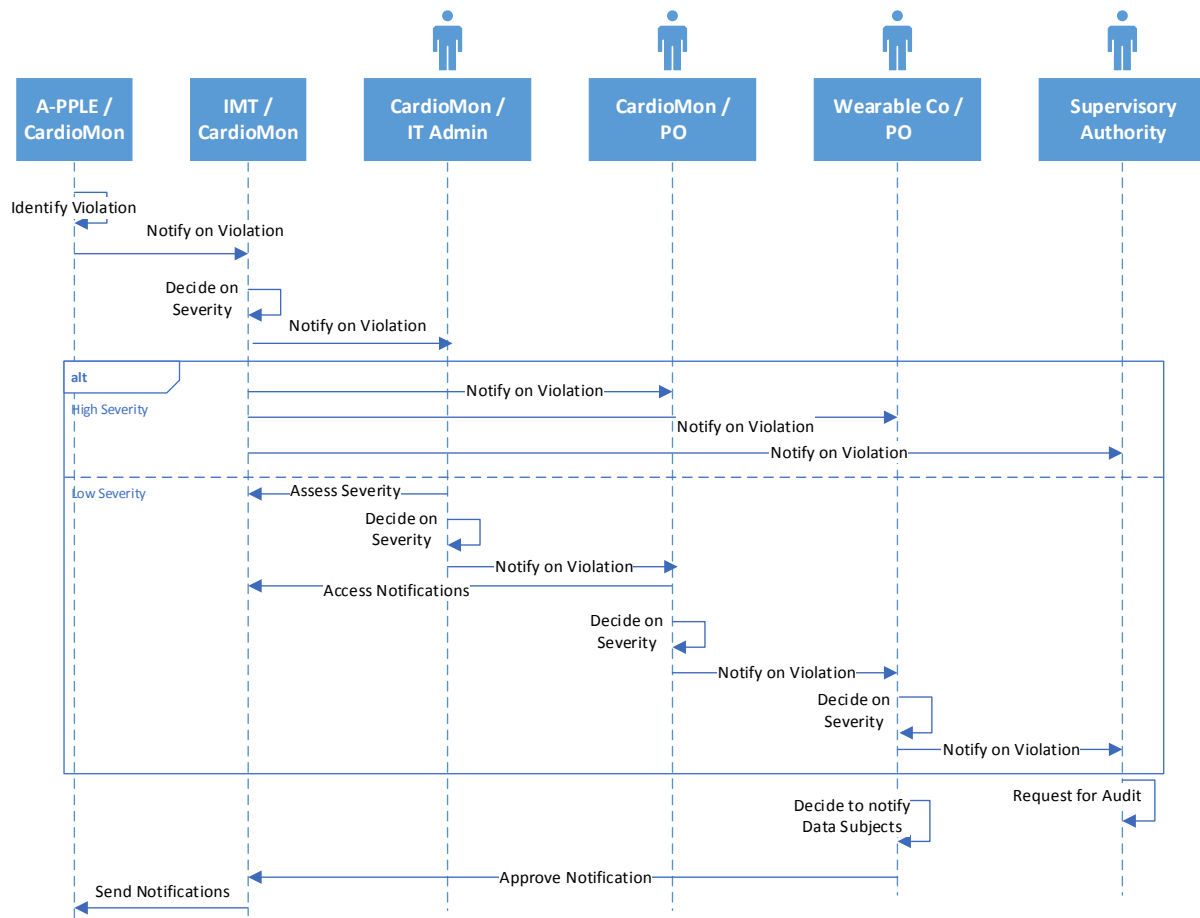


Figure 18: The process for the implementation of the notification accountability support services of corrective mechanisms

In the same way, when a notification for a Cloud Subject is available the process for implementing the remediation accountability support service is activated. This is shown in Figure 19.

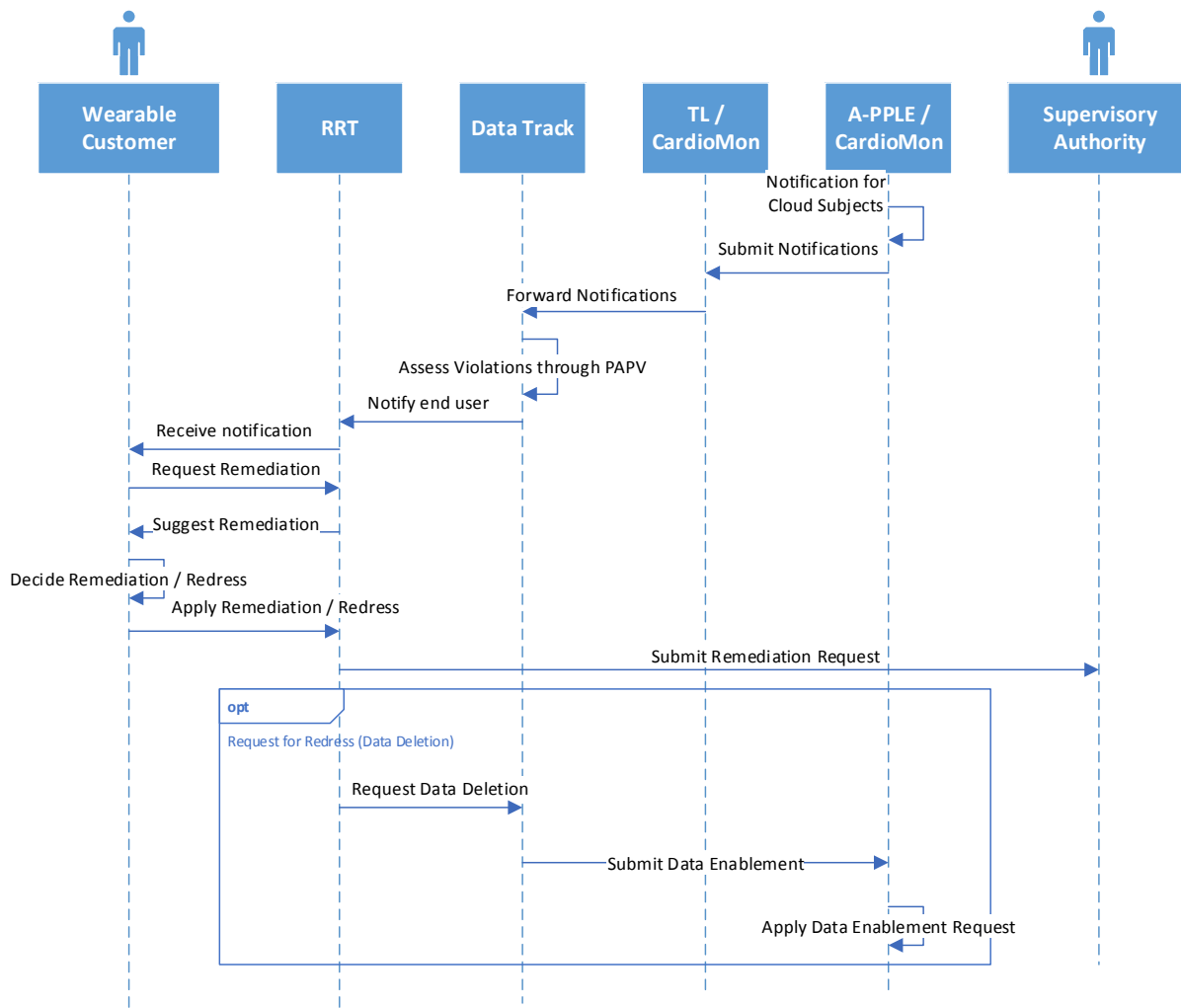


Figure 19: The process for the implementation of the remediation accountability support services of the corrective mechanisms

The notification on a specific incident reaches the end users (the wearable customers in the case of the Wearable Service), through A-PPLE. RRT is the respective front end tool to receive the incident notifications (through DT) and present them to the end users, along with a list of potential remediation actions. RRT, also, supports the end users in implementing specific remediation and redress.

This accountability support service has not been integrated in this First Prototype.

## 4 Presentation of the Wearable Use Case

This section exploits the description of the use case in Section 2 and the current status of the A4Cloud integration work, as presented in section 3, to present the evolution of the wearable use case demonstration. As such, this section selects a period in time to present the use of the Accountability Framework (as mentioned in Section 2.3, this is the time that CardioMon decides to develop and operate the Wearable Service), but it starts with the background information on what has supposed to have happened before this landmark for the sake of completeness.

### 4.1 The history of the scenario

As we presented in Section 2, the establishment of the different (cloud) service providers is performed in various time scales. Although a different order may happen and still be valid for our case, we consider the following time schedule, being evolved around January 2015.

By end of 2013, DataSpacer starts operating as an independent IaaS Cloud Provider, offering cloud storage and computation services out of a number of datacentres located in different geographical locations globally. Those datacentres are governed by different regulatory frameworks based on their location. In this use case, we assume that DataSpacer can allocate storage resources in Europe and US. Since DataSpacer is going to collaborate with cloud providers hosting any kind of personal data, this provider has to implement by default security and privacy mechanisms, while the relevant accountability tools, namely DTMT and AAS, have to be deployed to enable DataSpacer providing verification on their data handling processes upon ad-hoc requests from the collaborating cloud service providers or the governing Cloud Supervisor Authorities and Auditors.

Close to the summer of 2014, Map-on-Web starts its operation as a SaaS provider for delivering various data management solutions over large data streams, including data aggregation and smart visualisation. Data aggregation enables categorising the provided data streams, according to a specific criterion and calculate their mean values on a given timescale. Data visualisation includes the depiction of maps in order to deliver intuitive visualisation to the consumers of the analysed data streams. However, Map-on-Web does not provide any restrictions on the kind of data being processed by this cloud service or whether this data is temporarily or permanently hosted on the Map-on-Web side. Thus, Map-on-Web follows the Accountability Lifecycle steps to be able to be accountable to any future customer for their data handling procedures. At this point, Map-on-Web decides to operate their cloud deployment over the infrastructure provided by DataSpacer.

By the end of 2014, CardioMon delivers an in-house development for a Wearable Service, which serves potential customers to deploy their own wearable platform services. This is the case of the Wearable Co, which is preparing to procure a wearables software service (such as the CardioMon Wearable Service), as part of launching their new line of wearable devices early 2015. Due to the expected traffic load from the Wearable Co and other potential customers, the management board of CardioMon decides to start their business in the cloud. In that respect, the management board assigns the task of researching the market and selecting a cloud infrastructure provider to the IT admin and the Privacy Officer of CardioMon. To this end, these actors need to examine all the legal terms and conditions that govern the operation of such a business to be compliant to the local legal framework and design their policy in a way that the appropriate accountability mechanisms are in place from the collaborating cloud provider(s).

On top of that, the CEO of the Wearable Co assigns the respective Privacy Officer to investigate on accountable cloud service providers capable of providing the required Wearable Service. The choice needs to consider a lot of parameters, while the operation of the Wearable Service has to implement the respective accountability measures, which would enable the Privacy Officer of the Wearable Co to select a provider like CardioMon and constantly monitor their data handling practices.

The next sections demonstrate how CardioMon deploys their Wearable Service in the cloud in an accountable way and how the Wearable Co agrees with CardioMon to operate an instance of the Wearable Service for them, in the light of the data protection regime.

## **4.2 Analysing and designing the Wearable Service**

This section describes how the accountability framework, the A4Cloud Reference Architecture and the respective tools are demonstrated in the case of the Wearable Service, when CardioMon and the Wearable Co decide to introduce this service into the market. The demonstration of the design and development of the Wearable Service follows the accountability lifecycle processes (functional elements) of Figure 3 and is being evolved along the accountability support services.

We make the following assumption: although CardioMon and the Wearable Co come into business in different time windows, for the sake of demonstration, we consider that CardioMon and the Wearable Co collaborate on the same time frame to end up with the analysis and design phase.

### **4.2.1 The perspective of CardioMon**

#### **CardioMon Accepts Responsibility**

CardioMon understands the processes that the Wearable Service should implement, as shown in Table 1, and the type and sensitivity of the personal data involved in these processes, like the ones presented

in Table 2. We make the assumption that CardioMon aims to develop only those UI functionalities of Table 1 that refer to the wearable customers, but the exact data to be considered are left as part of the Wearable Service instantiation for a specific customer, which is the Wearable Co in our case. By doing so, CardioMon decides to start their business in a specific location (Greece), which is governed by a certain regulatory framework (the Greek Data Protection Regulation). The latter refers to high level obligations that CardioMon should comply with, as a cloud SaaS provider performing data processing on personal data. These obligations have already been described in [2] and are summarised in Table 8 of Section 8.2 of the Appendix.

### **CardioMon Identifies Controls**

By accepting responsibility for developing and operating the Wearable Service, CardioMon seeks for cloud providers, to which specific functional aspects of the Wearable Service can be subcontracted. More specifically, CardioMon investigates existing cloud providers to decide on which providers must be selected for collaboration so that they facilitate the needs for i) map visualisations on large data sets and ii) cloud storage. These functionalities must be provided subject to specific security and privacy requirements, which CardioMon introduces as selection criteria. These requirements derive from the fact that CardioMon has to comply with the Regulations and the ethical stance of the organisation to establish a certain level of trust to their customers. Moreover, these requirements refer to the ability of selected cloud providers to be accountable to CardioMon for the list of obligations deriving from the Greek Regulation (see Section 8.2) and implement specific mechanisms on who is accessing, viewing and processing the data that CardioMon will share with these providers. Such requirements include access control, supported encryption algorithms, data integrity checks, mechanisms for data retention and corresponding physical location of their data processing procedures.

#### *Use of COAT*

In order to implement the relevant functional accountability element, CardioMon uses COAT to select the appropriate cloud IaaS provider, which will undertake to implement the cloud storage requirements for hosting personal data, like the ones presented in Table 2. In that respect, the Privacy Officer of CardioMon loads the UI of COAT and selects the location of their business ("Greece") and the type of the COAT end users ("business"). By doing so, the page shown in Figure 20 is presented, in which the Privacy Officer of CardioMon selects the storage type for an Infrastructure as a Service requirement.



## Please indicate your requirements

What types of services do you need?

| Software<br>as a service  | Platform<br>as a service   | Infrastructure<br>as a service   | Other Services  |
|---|--|--|---|
| <input type="checkbox"/> Billing<br><input type="checkbox"/> CRM (Customer Relation Management)<br><input type="checkbox"/> Collaboration<br><input type="checkbox"/> Content Management<br><input type="checkbox"/> Digital Media<br><input type="checkbox"/> Document Management<br><input type="checkbox"/> ERP (Enterprise Resource Planning)<br><input type="checkbox"/> Emails and Office Productivity<br><input type="checkbox"/> Financials<br><input type="checkbox"/> Human Resources and Sales<br><input type="checkbox"/> Manufacturing<br><input type="checkbox"/> Order Management<br><input type="checkbox"/> Portals/Search<br><input type="checkbox"/> Social Network<br><input type="checkbox"/> Utilities/Management | <input type="checkbox"/> Application Deployment<br><input type="checkbox"/> Business Analysis<br><input type="checkbox"/> Business Intelligence<br><input type="checkbox"/> Databases<br><input type="checkbox"/> Development & Testing<br><input type="checkbox"/> Networks Operations<br><input type="checkbox"/> Open and Custom Clouds Platforms<br><input type="checkbox"/> Web Hosting | <input type="checkbox"/> Backup & Recovery<br><input type="checkbox"/> Communication<br><input type="checkbox"/> Computing<br><input type="checkbox"/> Infrastructure Service Management<br><input checked="" type="checkbox"/> Storage<br><input type="checkbox"/> Virtualisation | <input checked="" type="checkbox"/> Integration<br><input type="checkbox"/> Metadata<br><input type="checkbox"/> Security<br><input type="checkbox"/> Service-bus |

*Figure 20: CardioMon Privacy Officer using COAT to select the target service type*

As a first step, the Privacy Officer (PO) of CardioMon sees the first matched options, based on the type of services selected. Elaborating more on the CardioMon's privacy and security requirements, the PO navigates to the view shown in Figure 21. Through this view, the PO of CardioMon makes specific selections on the allowable geographical locations for data storage, backup and processing, use of encryption algorithms, etc. During this interactions, COAT keeps on filtering the results until the PO of CardioMon has finally found the necessary matches for the listed requirements.

One of the matching results is DataSpacer, which the PO of CardioMon decides to select and navigate to the "more info" option and review the features supported by this provider, along with the IT administrator of CardioMon, and a summary of the DataSpacer offered contract, as shown in Figure 22.

The same approach is used by the PO of CardioMon to select Map-on-Web as the appropriate SaaS provider to offer map visualisations.

## Cloud Offerings 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

What kind of Encryption





- ☐ Strong 2014 or better
- ☐ 256bit SSL
- ☐ SSL
- ☐ Client-Side Encryption
- ☒ Any

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

- ☐ Yes
- ☐ No

## 5 Matched Offers





Cirrus Thinking €10.00/Month

client-side encryption

[More info](#) [Go to offer](#)





Dataspacer €7.50/Month

1

[More info](#) [Go to offer](#)


Kar €10.00/Month

256bit ssl

[More info](#) [Go to offer](#)





€5.02/Month



strong 2014 or better

[More info](#) [Go to offer](#)

Wuala €9.99/Month

client-side encryption

[More info](#) [Go to offer](#)

Do you want Encryption?

Data protection authorities recommend that when you store and transmit personal information, the loss of which could cause damage or distress to individuals, you should protect this data using encryption. Encryption is designed to guard against the data being compromised and encryption of personal information is considered to be in accordance with good security personal information.

Figure 21: CardioMon Privacy Officer using COAT to select requirements

**Business Questionnaire**  
Please indicate your requirements

**Price Range**  
From: €0 To: €500

**Acceptable Storage Locations include**

- ☒ 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

**What kind of Encryption**

- ☐ Strong 2014 or better
- ☐ 256bit SSL
- ☐ SSL
- ☐ Client-Side Encryption
- ☒ Any

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

- ☐ Yes
- ☐ No

**dataspacer**

**Features**

|   |   |
|---|---|
| Service Price                                 | €7.50   |
| Processor Location                            | Greece  |
| Storage Location                              | Germany   |
| Backup  | Unlimited   |
| Court Jurisdiction                            | Greece  |
| Data Deletion (on Exit)                       | After a certain period of time  |
| Encryption Offered?                           | Yes   |
| Encryption Type                               |   |
| Provider Has Certification                    | No  |
| Law Enforcement Access                        | Hand over access to customer data to LE only if a valid subpoena/court order is given |
| Monitoring Options                            | Yes   |
| Ownership                                     | Data generated by the user remain the sole property of the customer                   |
| Notification of Security Breach?              | Yes   |
| Service Type(s)                               | Storage<br>Infrastructure Service<br>Management<br>Integration                        |
| Notification on change of Terms & Conditions? | Yes   |
| Subcontracting Used?                          | Yes   |
| Notification on change of Vendor?             | No  |

**Service Offers**

- €10.00/Month  
client-side encryption  
More info Go to offer
- €7.50/Month  
1  
More info Go to offer
- €10.00/Month  
256bit SSL  
More info Go to offer
- €5.02/Month  
strong 2014 or better  
More info Go to offer
- €9.99/Month  
client-side encryption  
More info Go to offer

Figure 22: CardioMon Privacy Officer inspecting the details of the DataSpacer contract

### Use of DPIAT

Going further to the “identify controls” element of the accountability lifecycle, the PO of CardioMon wants to assess the risks related to the selection of DataSpacer to serve the storage service type. In that respect, DPIAT is loaded (see Figure 23), in which the PO is given the option to take a Pre-screening questionnaire (consisting of 6 questions) to quickly assess whether PO needs the full Screening questionnaire (consisting of 56 questions) or not. Thus, the PO of CardioMon, first, selects the service provider under assessment, in this case DataSpacer.


Based on the result of the pre-screening questionnaire, the PO of CardioMon is consulted in taking the full screening questionnaire. Thus, in case that the result of the pre-screening questionnaire is like the one depicted in Figure 24, the PO is directed to the full Screening questionnaire (see an example in Figure 25).

## A4Cloud 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

— please choose a provider — 

#### 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](#)

Figure 23: DPIAT Landing Page

## A4Cloud Data Protection Impact Assessment Tool

### Questionnaire Results

Based on your answers, you have to complete the [Screening Questionnaire](#).

Please click the link to proceed

Figure 24: Report page of the Pre-screening questionnaire

## Screening Questions

[Save for later](#)


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.

### 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.*

- ☐ (Service) Delivery
- ☐ Account and/or Subscription Management
- ☐ Authentication and Authorization
- ☐ Advertising, Marketing, and/or Promotion
- ☐ Banking and Financial Management
- ☐ Customization
- ☐ Communications Services
- ☐ Charitable Donations
- ☐ Education Services
- ☐ Government Services
- ☐ Healthcare Services
- ☐ News and Information- Arts and Entertainment
- ☐ Online Gambling
- ☐ Online Gaming
- ☐ Payment and Transaction Facilitation
- ☐ Responding to User
- ☐ Software Downloads
- ☐ Sales of Products or Services
- ☐ Surveys and Questionnaires
- ☐ Search Engines
- ☐ State and Session Management
- ☐ Web Browsing

Figure 25: Example view of the screening questionnaire taken by the Privacy Officer of CardioMon

After answering the questions, the PO of CardioMon gets a final impact assessment report, which gives guidance related to three areas: Project-based Risks (assessed by the answers from the questionnaire), CSP-based risks for DataSpacer (assessed by the information gathered from the CSA Star Registry about DataSpacer), and any more related information. The user is, also, given the overall risk, which is calculated from both the Project-based risks and the CSP-based risks.

The same approach is used by the PO of CardioMon to assess the risks associated with the selection of Map-on-Web as the appropriate SaaS provider to offer map visualisations.

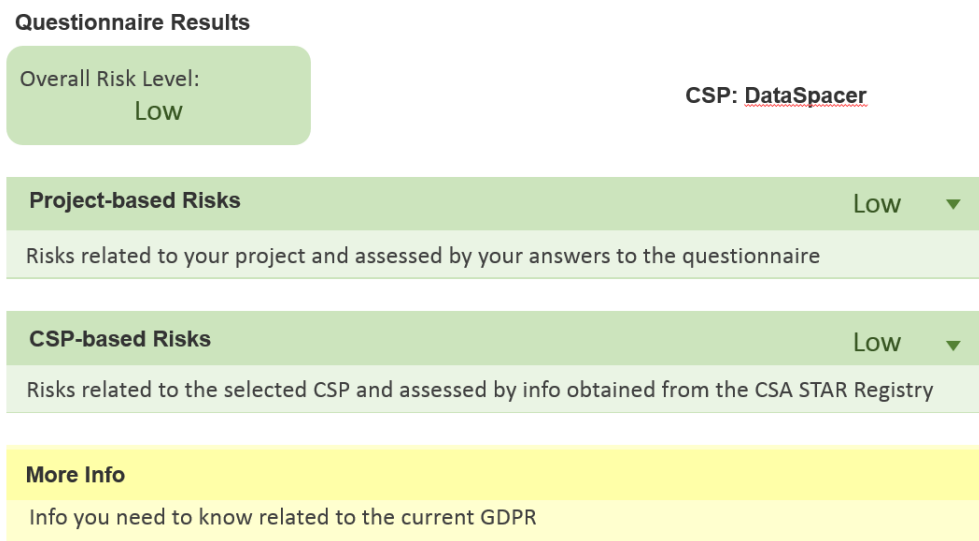


Figure 26: Example DPIAT report for the risk assessment on DataSpacer

#### 4.2.2 The perspective of the Wearable Co

Following the same practice, the Privacy Officer of the Wearable Co accepts responsibility for offering the Wearable Service through CardioMon cloud service and delivers the processes shown in Table 1 for both their wearable customers and for the Wearable Co employees. This means that the Wearable Service being offered by CardioMon is instantiated for the sake of the Wearable Co to provide additional functionalities. The collaboration of the Wearable Co with CardioMon, also, involves the exact identification of personal data that should be involved in this instance of the CardioMon service, as they are shown in Table 2. Again, the Wearable Co is subject to the Greek Regulation and the high level obligations depicted in Table 9 of Section 8.2 of the Appendix.

Based on these obligations, the Wearable Co ends up with the list of privacy and security requirements that should be satisfied during the development of the Wearable Service. The requirements stem from legal and normative obligations of both CardioMon and the Wearable Co and they refer to UI functions presented in Table 1. In this first prototype, we have implemented a subset of these functionalities, which are summarised in Table 6. In this table, we elaborate on the accountability related requirements and provide the source of the respective obligations (either being derived from the legal framework or the adoption of accountability from an ethical perspective).

Table 6: The Wearable Service UI level functionalities of the wearable customer and accountability related requirements<sup>5</sup>

| Title of Functionality         | Accountability Related Requirement  | Source from CardioMon Obligations                                 |  |
|--------------------------------|---|---|--|
|                                |   | Legal Obligation  | Normative Obligation   |
| <b>Create Customer Profile</b> | The Wearable Customers must accept a consent form on being aware of the type of personal data collected, processed and stored in the cloud. | C1, W1, W2, W3, W4, W5, W7, W9, W10, W11, W12, W13, W14, W15, W17 | compliance with privacy policies<br>monitoring of data practices |
| <b>Log in</b>                  | All users must be subject to access and usage control rules, concerning personal data access  | W6, W8, W11   | compliance with privacy policies                                 |

<sup>5</sup> This table makes reference to the CardioMon obligations in Table 8.

| Title of Functionality                   | Accountability Related Requirement   | Source from CardioMon Obligations |  |
|--|--|-----------------------------------|--|
|  |  | Legal Obligation                  | Normative Obligation   |
|  | defined in the accountability policy for all the data of Table 2   |                                   | monitoring of data practices   |
| <b>Manage Profile</b>                    | An accountability policy should define that the Wearable Customers can read / update / delete the following data: username, password, user id, display name, gender, age, height, weight, sugar level, blood pressure, heartbeat rate, training activity, country        | W5, W6, W8, W11                   | compliance with privacy policies<br>monitoring of data practices   |
| <b>Submit Real-time Information</b>      | An accountability policy should define that only the wearable device of a wearable customer can submit sugar level, blood pressure and heartbeat rate  | W5, W8, W11                       | compliance with privacy policies<br>monitoring of data practices   |
| <b>Update activities</b>                 | An accountability policy should define that the Wearable Customers must be able to create and modify an activity profile per day, for all training activities  | W5, W6, W8, W11                   | compliance with privacy policies<br>monitoring of data practices   |
| <b>Request Real-time Information</b>     | An accountability policy should define that only the Wearable Customers must be able to read their sugar level, blood pressure and heartbeat rate  | W8, W11                           | compliance with privacy policies<br>monitoring of data practices   |
| <b>View active users</b>                 | An accountability policy should define that the Wearable Co employees and the IT Admins of CardioMon have restricted access to the personal data of the Wearable Customers and can only read the following personal data: user id, display name, gender, age and country | W8, W11                           | compliance with privacy policies<br>monitoring of data practices<br>privacy-by-default                               |
| <b>Request Statistical Visualisation</b> | An accountability policy should define that Map-on-Web can only read the following personal data: age, country, sugar level, blood pressure and heartbeat rate   | C1, W8, W12                       | personal data minimization<br>compliance with privacy policies<br>monitoring of data practices<br>privacy-by-default |
| <b>Request data handling compliance</b>  | A tool has to be implemented to enable analysis of evidence records for specific audits tasks  | C2, C3                            | compliance with privacy policies<br>monitoring of data practices   |



| Title of Functionality                              | Accountability Related Requirement   | Source from CardioMon Obligations |   |
|---|--|-----------------------------------|---|
|   |  | Legal Obligation                  | Normative Obligation  |
| <b>Receive alerts on excessive wellbeing values</b> | An accountability policy should define that only the Wearable Customers have access to the alerts with respect to their wellbeing values exceeding thresholds  | W8, W11                           | personal data minimization<br>compliance with privacy policies<br>monitoring of data practices  |
| <b>Receive policy violation alert</b>               | An accountability policy should define that all the wearable customers, the IT admin of CardioMon and the PO of the Wearable Co must be notified of any policy violation incidents   | C2, C3, W7, W16                   | compliance with privacy policies<br>monitoring of data practices<br>informing about policy violations<br>informing about privacy preferences violations<br>remediation in case of damages |
| <b>Receive transfer violation alert</b>             | An accountability policy should define the allowable location for storing and processing personal data collected by the Wearable Service and that all the wearable customers, the IT admin of CardioMon and the PO of the Wearable Co must be notified in case of any transfer violation incidents | C2, C3, W17                       | compliance with privacy policies<br>monitoring of data practices<br>informing about policy violations<br>informing about privacy preferences violations<br>remediation in case of damages |
| <b>Receive breach notification</b>                  | An accountability policy should define that any breach notification should be notified to all the wearable customers, the IT admin of CardioMon and the PO of the Wearable Co  | C2, C3, W16                       | compliance with privacy policies<br>monitoring of data practices<br>informing about privacy preferences violations<br>remediation in case of damages                                      |

#### 4.2.3 Implementation of Measures

Through the analysis and design of the Wearable Service, as presented in the previous paragraphs, CardioMon and the Wearable Co can negotiate on a privacy policy that should be presented in two forms, the lawyer readable privacy policy (see Section 8.3), which is agreed between the privacy officers of the Wearable Co and CardioMon, and the machine readable representation of this policy (as it is presented in Section 8.4) and refers to the form of the policy, which will be enforced by the A4Cloud

respective policy engine tool the A-PPLE instance of CardioMon. Currently, the machine readable policy is prepared by the Security Expert of CardioMon.

In order to come up with the policy definition, we, here, provide an example on how the accountability related requirements are translated to machine readable accountability policy rules. We focus on the function about viewing the active users from Table 6, which raises the requirement for an accountability policy, which restricts the read access rights of the Wearable Co employees only to a subset of the wearable customers' personal data, namely user id, display name, gender, age and country. This is implemented through the following part of the policy file of Section 8.4:

[illegible]

```

        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">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>

```

In a similar way, in the data handling policy part, a specific rule on the need to ask the Wearable Customers for giving their consent for processing their personal data by CardioMon (as part of the Create Customer Profile function of Table 6), like the following:

```

<ob:Obligation elementId="a-ppl_rule_6">
    <ob:TriggersSet>
        <ob:TriggerOnUserRegistration />
    </ob:TriggersSet>
    <ob>ActionRequestConsent />
</ob:Obligation>

```

At this point, the machine readable policy of Section 8.4 is agreed between CardioMon and the Wearable Co and CardioMon starts instantiating the Wearable Service for this cloud customer. Based on the analysis presented in Sections 4.2.1 and 4.2.2, the instance of the Wearable Service, which serves the Wearable Co business, should expose a Web User Interface implementing the functionalities of Table 6 for two application roles, namely the wearable customer and the employee.

In the backend, CardioMon and their third parties, that is Map-on-Web and DataSpacer, are subject to the deployment of the measures agreed between CardioMon and the Wearable Co in order to ensure security and privacy. CardioMon is the actual orchestrator of this process, as this actor is accountable to the Wearable Co for the legal and normative obligations of themselves and their third parties.



Each role in this cloud chain should provide an account to the accountee organisation that all the appropriate measures have been safeguarded with respect to the agreed accountability policy. At the deployment phase, the account includes proofs that accountability policy is properly configured in all parts of the cloud service chain. The latter could be realised through the use of the Assertion Tool, but for this first prototype we assume that this is already done in a manual way.

In that respect, for example, the action for checking the proper enforcement of DTMT policy on the DataSpacer side is an account for CardioMon that the specific data transfer requirement is achieved. At this step of the lifecycle, CardioMon submits the part of the accountability policy that refers to data location handling procedures and requests from DataSpacer to run a relevant test scenario and provide the results of this validation phase.

Another account that CardioMon is collecting from the cloud infrastructure refers to the action for checking the proper enforcement of the accountability policy on the Map-on-Web side. This is an account for CardioMon that the specific data protection requirements are achieved.

In a similar way, on the Wearable Co side, the action for checking the proper enforcement of the accountability policy on the CardioMon side is an account for the Wearable Co that the specific data access, data retention and deletion and data transfer requirements of Table 6 are achieved.

Currently the process for gathering the account on the proper implementation of measures is performed manually, but, in the next prototype, this is to be done through the Assertion Tool.

### 4.3 Operating the Wearable Service

Before entering the operational phase of the Wearable Service for the Wearable Co, this cloud customer may proceed with the software customisation of the CardioMon cloud service. The customisation may refer to the (de-)activation of specific functionalities offered by the Wearable Service and implementation of a completely new front end, which enables the interaction of the Wearable Customers with the Wearable Service. Following this, the Wearable Co is ready to announce the operation of the Wearable Service, hosted by CardioMon. Thus, the description in this section refers to the perspective of CardioMon for serving the requirements of the Wearable Co.

The Wearable Service of the Wearable Co is a Web application (see Figure 28 for the home page), which distinguishes between two application roles, namely:

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



Figure 28: The home page of the Wearable Service

#### 4.3.1 The operations of the Wearable Customer

The Wearable Service offers the following main pages (UI screens) for the wearable Customer, which implement the functions of Table 6:

- Registration Page: this page enables a Wearable 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 Customer to be authenticated to the service.
- Manage Profile page: this page enables a Wearable 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 Customer to retrieve an overview of their wellbeing 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 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 Customer to navigate to the overall statistics of the wellbeing 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 Customer, along with a set of screenshots visualising the pages that the Wearable Customer goes through.



From the home page (see Figure 28), the Wearable Customer selects the login button from the top right menu bar (highlighted by the orange dashed rectangular<sup>6</sup>). The login page is then displayed, as shown in Figure 29. 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'. In the 'REGISTERED USER' section, there are input fields for 'Username' and 'Password', a 'LOGIN' button (highlighted with an orange circle and a '2' in an orange box), and a 'Lost Password?' link. In the 'CREATE AN ACCOUNT' section, there is a paragraph of placeholder text and a 'CREATE AN ACCOUNT' button (highlighted with an orange circle and a '1' in an orange box).

Figure 29: The login page of the Wearable Service

The screenshot shows a web page titled 'Privacy Policy'. The content is organized into several sections: 'Privacy Policy of Wearable Company' (with a paragraph about the purpose of the form), a paragraph about consent, 'About the Wearable Company' (with a paragraph about the company's role and a paragraph about its location), 'About the purposes for which your data will be processed' (with a paragraph about data usage), and a final paragraph 'We will use your personal information to:'.

Figure 30: The consent form that the wearable customer needs to accept during the registration phase

<sup>6</sup> Orange highlighted shapes (ellipsis or rectangular) in solid or dashed lines are used in the screenshots to focus on a specific function on the respective Web page.



During registration, the Wearable 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 of Section 8.3 and takes the form of Figure 30. After accepting this form, the wearable customer is prompted to fill in the personal data of the profile (see Figure 31), which are a subset of those presented in Table 2 and namely 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 application). Using the declared credentials, the wearable customer can select option 2 from Figure 29 to log in to the Web application.

Registration form

PLEASE FILL THE FOLLOWING FIELDS

Username  
v.tountopoulos

Password  
.....

Retype Password  
.....

Display Name  
Vasilis Tountopoulos

Email  
v.tountopoulos@atc.gr

*Figure 31: The Registration page of the Wearable Service*

Upon successful registration and login, the Wearable Customer is shown the screen shown in Figure 32. Through this page, the user either selects option 1 for real time monitoring of the collected wellbeing 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 32, the Wearable Customer retrieves the view of Figure 33, which displays the aggregated value of the wellbeing 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 32, 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 34.

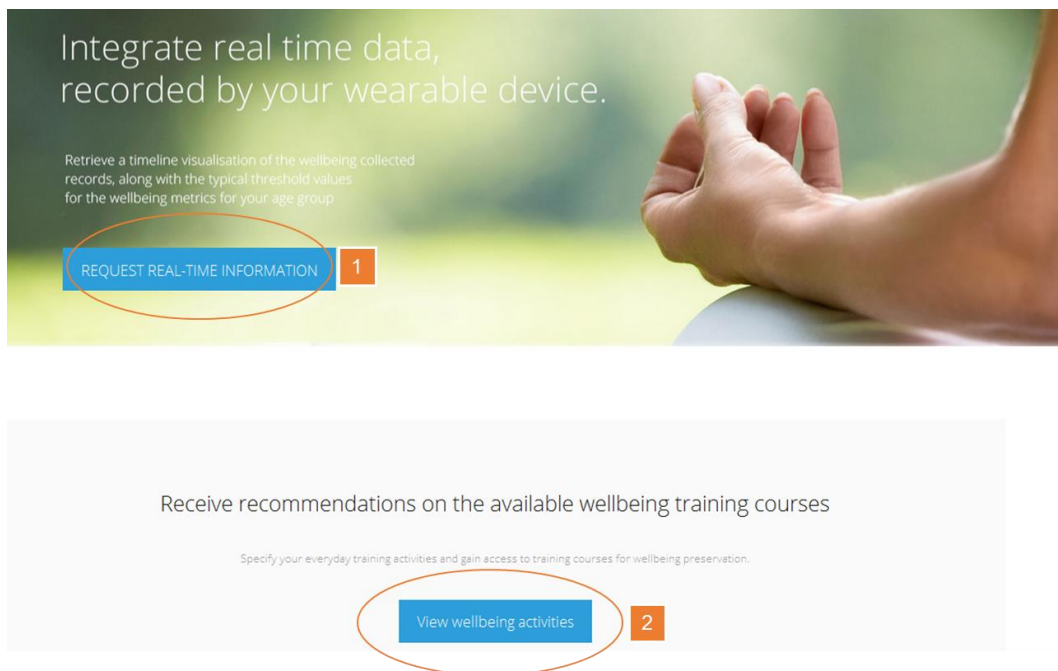


Figure 32: The first page of the logged in Wearable Customers

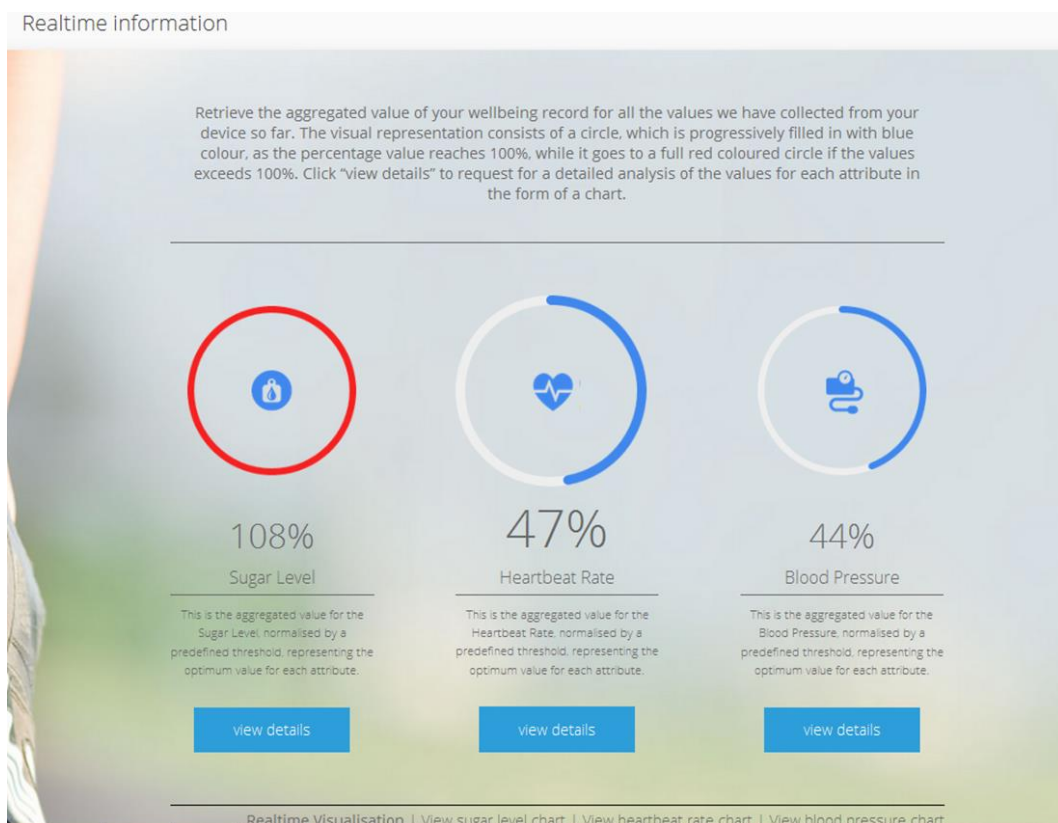


Figure 33: The real time information page of the logged in Wearable Customers

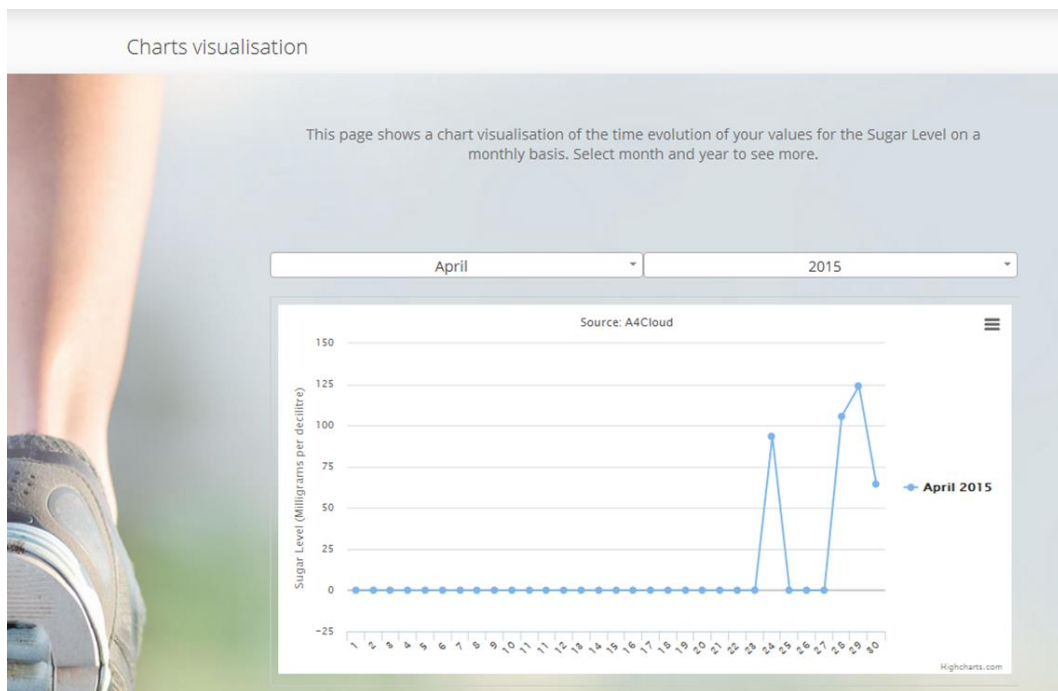


Figure 34: The Wearable Service page for chart visualisation of the real time information for the logged in Wearable Customers

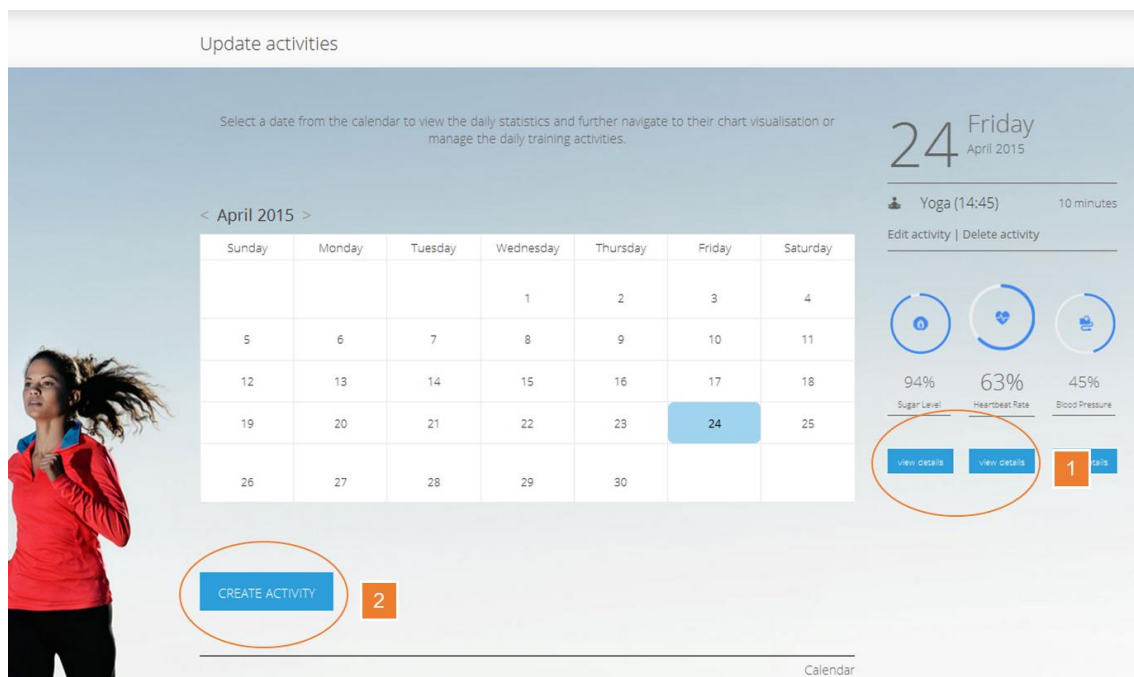
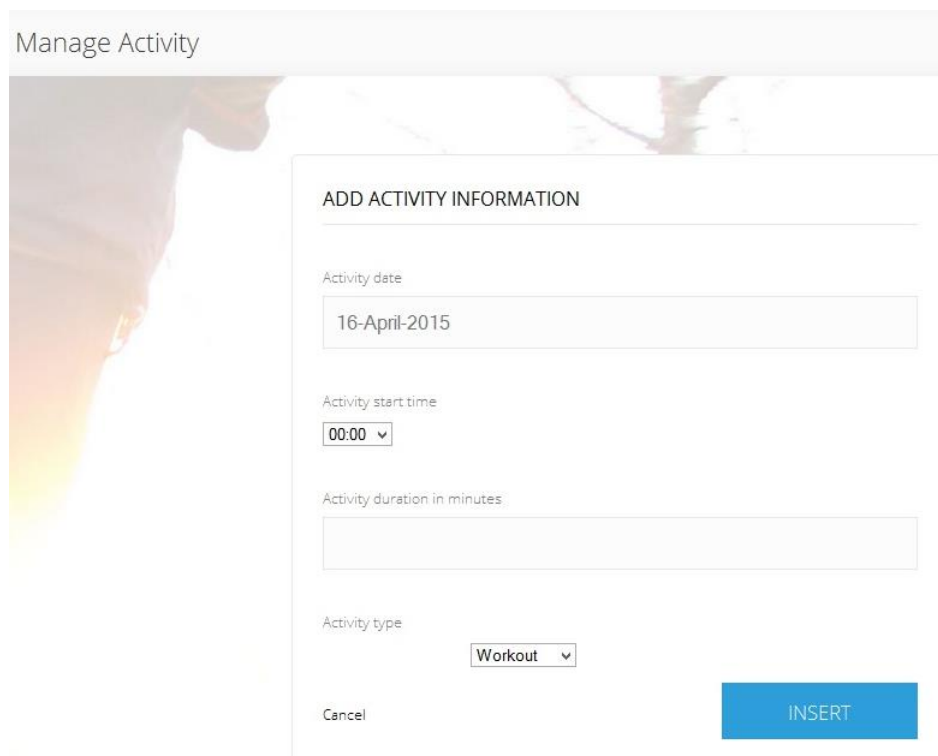


Figure 35: The screen of the Wearable Service to manage wellbeing activities

Following option 2 of Figure 32, the Wearable Customer can manage his/her daily activities. To this end, the Web application displays the picture of Figure 35, 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 wellbeing 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 34, but for personal data collected on the selected date), or manage the daily training activities.
- Option 2: create a new activity as per Figure 36



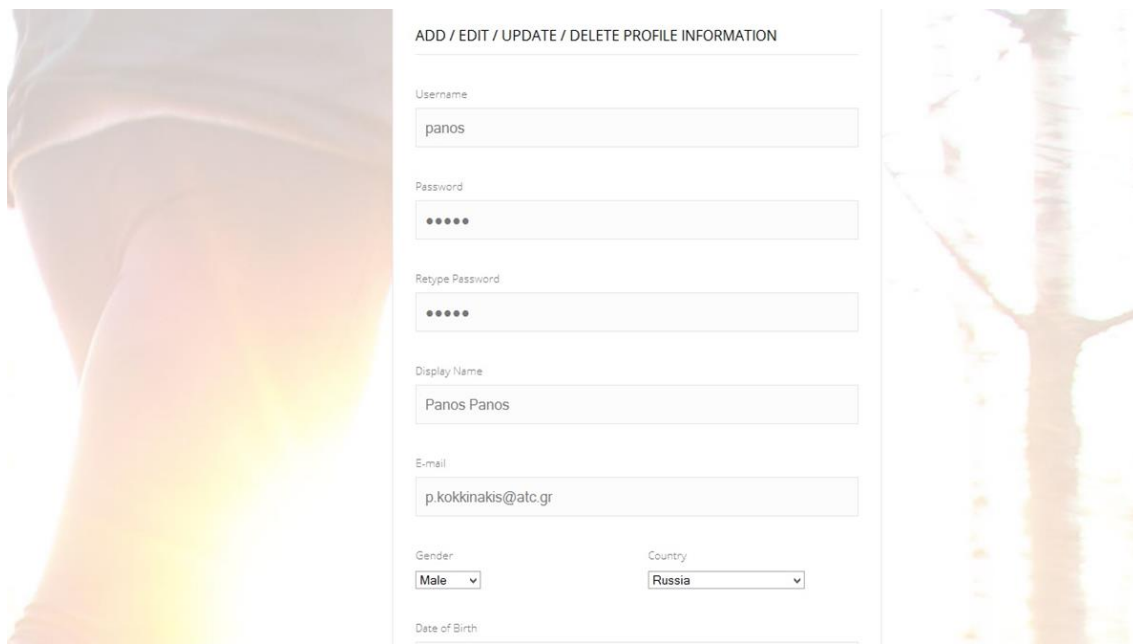
The screenshot shows a web interface titled "Manage Activity". It features a form with the following fields and controls:

- ADD ACTIVITY INFORMATION** (Section Header)
- 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.

*Figure 36: Managing activities in the wearable Service*

In all pages, the Wearable 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 37.

Through the same menu bar, the Customer has access to the Statistics Page. This is an additional page, which integrates the wellbeing records from all the Customers registering to the Wearable Co. At this point, the request from the Wearable Service in CardioMon is forwarded to the MapOnWeb side. The latter is responsible for getting the relevant information from CardioMon and deliver two views: i) one similar to Figure 33, but aggregating the data coming from all the Wearable Customers and the detailed map visualisation of Figure 38. The latter distinguishes the wellbeing 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 Customer that this data belongs to (as per the relevant part of the machine readable policy of Section 8.4. 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 37: The Manage Profile page of the Wearable Service

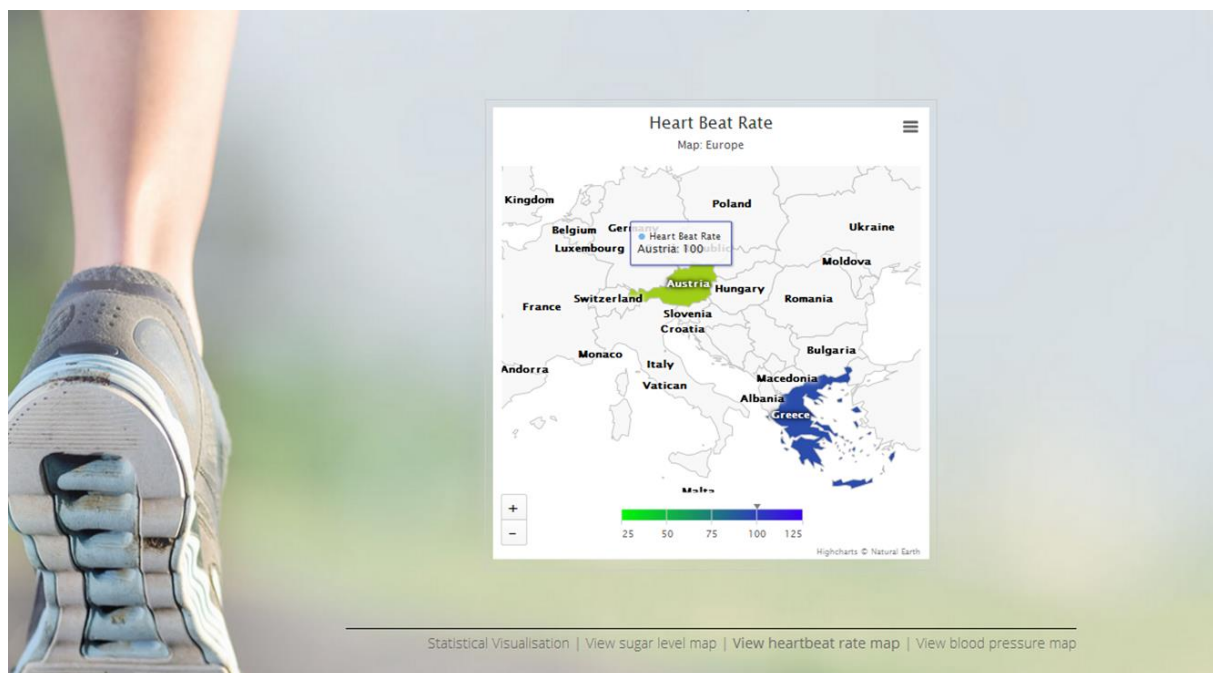


Figure 38: The statistical Map visualisation page of the Wearable Service

#### 4.3.2 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 Table 6:

- Log-in Page: this page enables the Employee to be authenticated to the service.
- Manage Profile page: this page enables a Wearable Customer 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.
- Alerts page: this page enables the Employee to aggregate the alerts generated by the operational environment to browse through the description and the details of each alert.
- Request map visualisation page: This page enables the Employee to navigate to the overall statistics of the wellbeing 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.

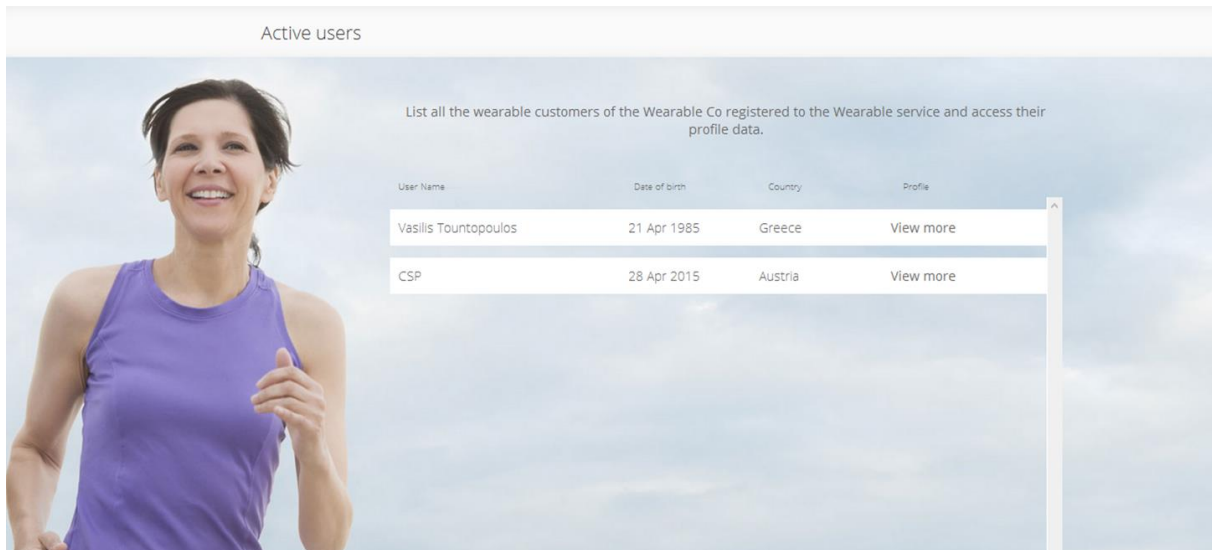


Figure 39: The first page of the logged in Employees

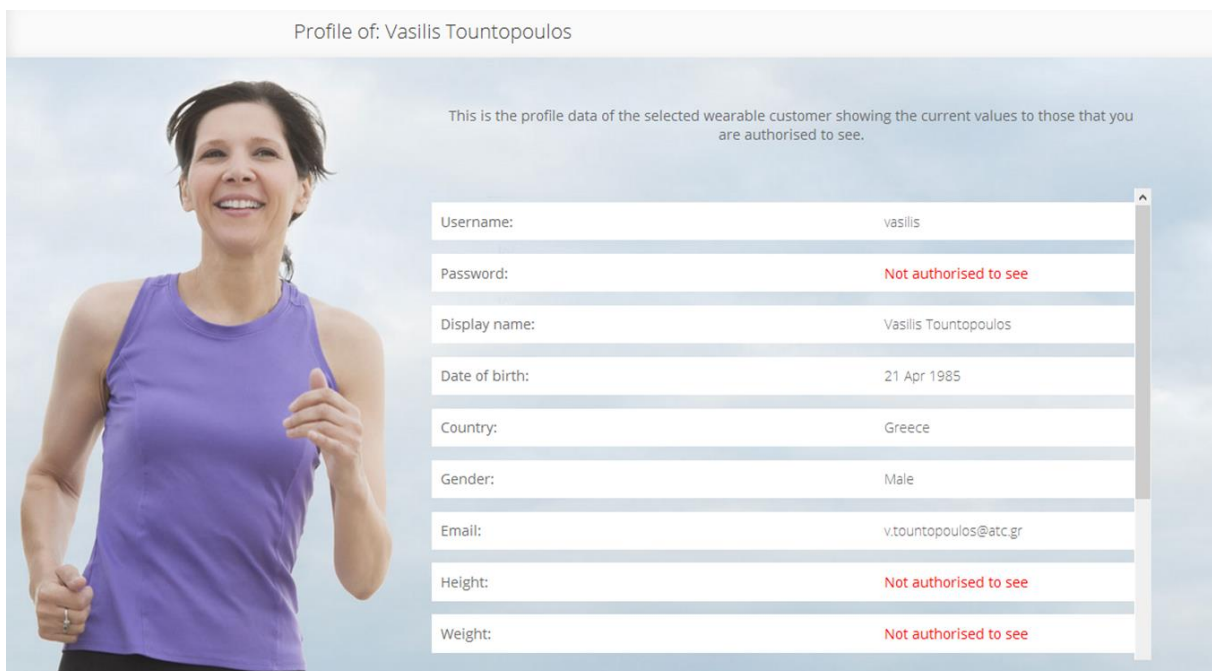


Figure 40: An employee viewing the profile of a wearable customer



From the home page (see Figure 28 – shared view with the Wearable 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 29 (shared view with the Wearable Customer). It must be noted that the Web application assigns all the newly registered users as Wearable 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 39. Through this page, the employees can browse the whole list of the Wearable 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 40.

Again, in all pages, the Employee has access to some more pages from the menu bar in the top of the screen. From this menu and by pressing the “Alerts” button, the Employee can browse through the list of alerts received from the A4Cloud tools (through the A-PPLE instance of CardioMon), as shown in Figure 41. For the time being, the alerts are classified as transfer violation and policy violation alerts and the Employee can expand the alerts view to read through the details of each alert. The alerts are generated while we implement the incidents that should be handled by the A4Cloud tools, as explained latter in this document.

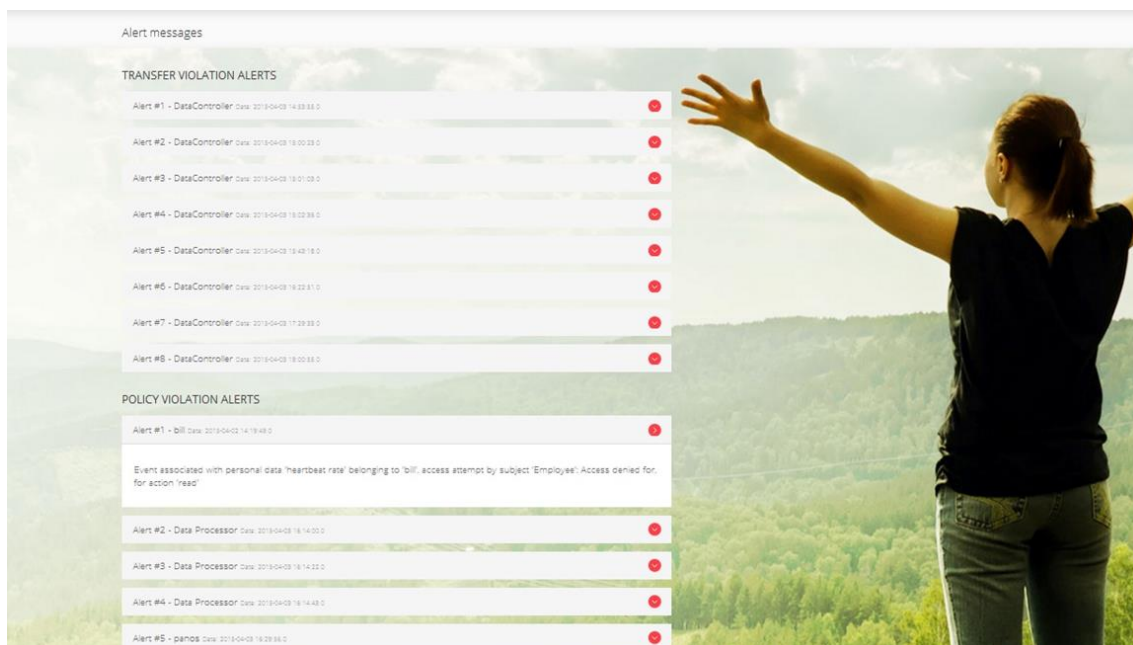


Figure 41: The alerts page of the Wearable Service

As in the case of the Wearable 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.

#### 4.4 Gathering Evidence

In the previous section, we made an introduction to the business operations of the Wearable Service for the two envisaged roles. At runtime, while the different actors access these operations, the relevant A4Cloud tools deployed as per Figure 9, generate and/or collect logs with respect to data protection actions arisen from the accountability policies. The evidence gathering phase of this application follows the sequence of actions depicted in Figure 14, Figure 15 and Figure 16, depending on which the time scale and cloud architecture layer we demonstrate the scenario.

As a first example for the implementation of the gathering evidence step in the Accountability Lifecycle of CardioMon, let's assume that the Wearable Customer visits the page viewed in Figure 34 for the attribute name blood pressure. In this case, the request for chart visualisation of the blood pressure values per month is forwarded to the A-PPLE instance of CardioMon to check the policy rules and accept or deny the request coming from this Data Subject. The policy checking in the A-PPLE instance of



CardioMon results in the generation of A-PPLE logs, following the sequence of Figure 14, but having the Wearable Customer as the triggering actor instead of the Employee. In a similar way, when the Employee accesses the page shown in Figure 39 and selects a user to request their profile data, the back end logic of the Wearable Service makes several PII requests to A-PPLE, one per PII data listed in Figure 40. For each PII request, the sequence of Figure 14 is followed either resulting in “accept or deny action” handler.

When the Wearable Customer requests the Statistics page in Figure 38, the Wearable Service forwards the request to Map-on-Web, which in turn asks for the wellbeing records from the A-PPLE instance of CardioMon. In this case, the AAS instance of CardioMon monitors the interactions between CardioMon and Map-on-Web on whether they happen through an encrypted way (e.g. https requests), as dictated in the policy. The client part of AAS logs the interaction as an evidence in the Evidence Store.

On a different scale, DTMT is used to monitor the operations at the DataSpacer layer. All infrastructure level functionalities are monitored to collect logs with respect to data transfers happening during the resource pooling and balancing functionalities of the cloud environment.

#### 4.5 Handling Exceptions

During the operation of the Wearable Service, abnormal behaviour may occur. For this case and in order to demonstrate the identification of incidents from CardioMon, we assume a number of incident scenarios referring to the violation of data protection rules, namely, inappropriate data access requests, application of data retention and deletion rules, unauthorised data transfers, service encryption vulnerability and unavailability. With these scenarios we aim to showcase the ability of the different A4Cloud tools to detect violations and raise incidents that should be handled through the notification and remediation accountability support services. The scenarios are analysed in the following.

##### *Incident Scenario 1 – Unauthorised Data Access*

In this scenario, we consider the functionality that the Employee accesses the profile of a selected Wearable Customer, as shown in Figure 40. According to the policy, the Employee has access only to a subset of the profile data for the customer. Thus, the request of the Wearable service to the A-PPLE instance of CardioMon results in A-PPLE raising a deny request response, logging this to the Evidence Store of CardioMon, as shown in Figure 14 (currently, A-PPLE is not integrated with Evidence Store, so for this first prototype the A-PPLE logs are maintained with this tool), and sending back to the UI a “404 unauthorised” message, as shown in Figure 40.

This incident should be handled as per Figure 18 for the remediation phase. Currently, the incident notification generated by the A-PPLE instance of CardioMon is populated to the alerts page of the Employee and the policy violations part (see Figure 41).

##### *Incident Scenario 2 – Inadequate Data Retention and Data Deletion*

During the normal operation of the Wearable Service, CardioMon performs regular backups by creating snapshot instances of the CardioMon VM image in DataSpacer. This is achieved through the IT admin of CardioMon accessing the dashboard of the OpenStack installation in DataSpacer and invoking the “create snapshot” functionality as shown in Figure 42.

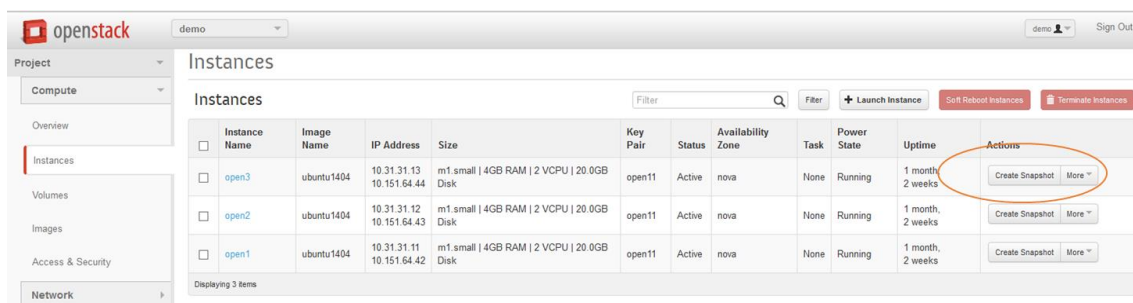


Figure 42: Creating a snapshot of the CardioMon VM through the OpenStack dashboard

By doing so, the relevant storage area allocated to CardioMon is backed up in this snapshot as well.

During the policy enforcement, one of the rules applied to the Wearable Service refers to the maximum period of time that the data collected for a Wearable Customer could be maintained by the A-PPLE instance of CardioMon. We assume that, for a Wearable Customer, this period expires and A-PPLE applies the data retention rule by generating the relevant logs as shown in Figure 15. However, an existing record of this Customer's data still resides in DataSpacer and can be accessed by CardioMon, through the snapshot created for backup purposes. Thus, although the policy rule is applied in the operational PII store of the CardioMon A-PPLE instance, the AAS instance of CardioMon detects the snapshot creation and generates an incident, as shown in Figure 15.

#### *Incident Scenario 3 – Unauthorised Data Transfers*

As mentioned earlier, the policy specifies that the data related to the Wearable Service of the Wearable Co must be processed and stored in the EU data center of DataSpacer. As shown in Figure 9 a specific data volume, is attached to the compute node, in which CardioMon resides in, thus in the EU data center of DataSpacer. Due to a hardware failure, the IT admin of DataSpacer accesses the OpenStack dashboard (see Figure 43) and detaches this data volume from Compute Node 1, attaching it to Compute Node 2. Subsequently, this results in data moving to a third party location (US in this case), which is not allowed by the policy.

This action is monitored by DTMT residing in the Controller Node of DataSpacer and identifies it as a potential violation. In turn, DTMT generates a notification and sends this to the A-PPLE instance of CardioMon (see the relevant process in Figure 16), since the potential data transfer violation refers to the data storage of CardioMon. The respective A-PPLE instance verifies the violation and produces an alert notification, which is, currently, populated to the UI of Employee, under the transfer violation alerts of Figure 41, for demonstration purposes.

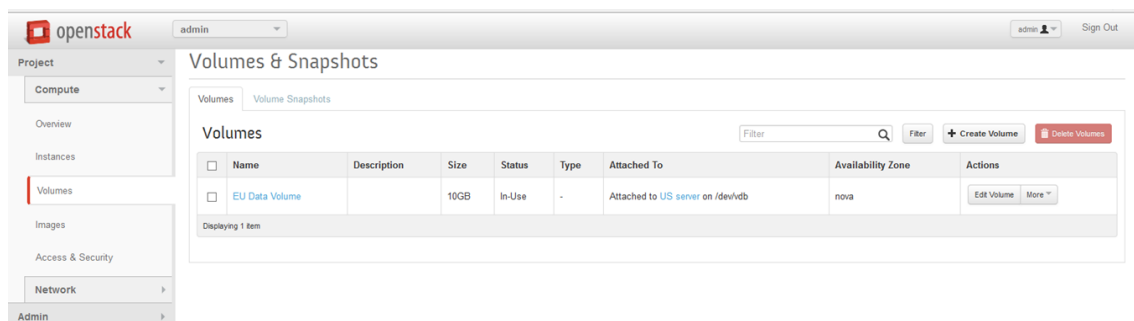


Figure 43: Attach-detach a data volume from a compute node

## 4.6 External Verification

At regular time intervals, CardioMon wants to verify their data processing practices. To this end, the AAS instance of CardioMon enables an Auditor connecting with the AAS Dashboard to perform audits.

An overview of the Dashboard for the AAS instance of CardioMon is presented in Figure 44. As seen there, the Auditor is given a quick overview of currently active audits and their corresponding evidence collection tasks as well as audit results if available. From this landing page, the auditor can quickly create new audit policies, have a detailed look at audit results and, if needed, request additional evidence records for further manual investigation.

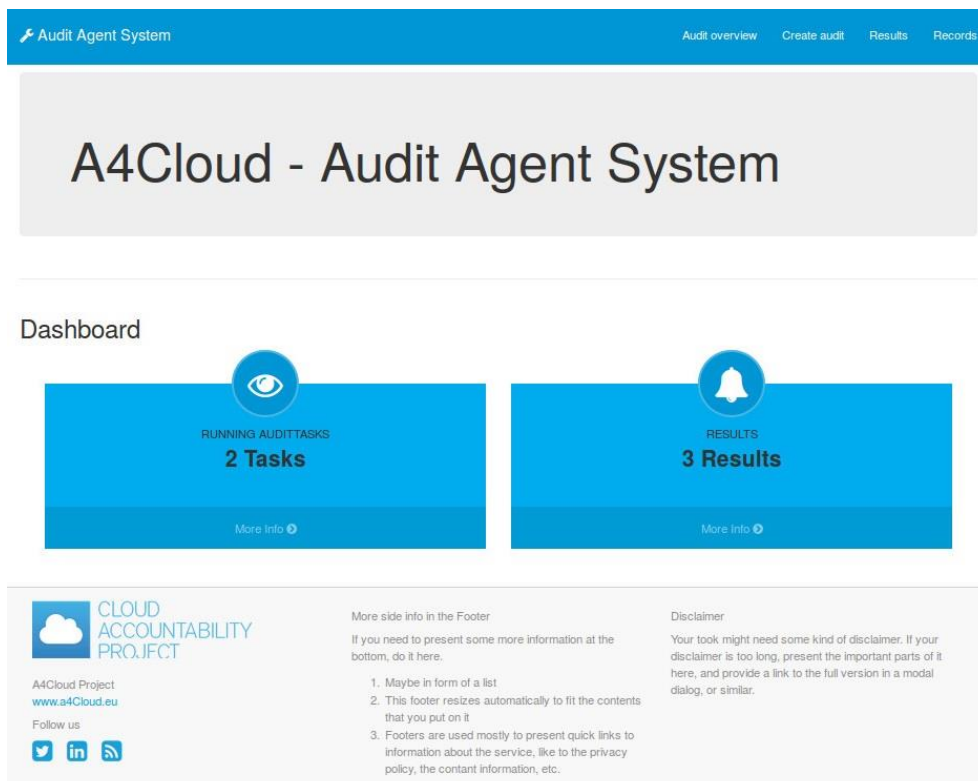


Figure 44: CardioMon AAS Dashboard Overview

In Figure 45, the dashboard for creating new audit policies and tasks is shown. In this case, the auditor has parsed the data handling parts of an A-PPL policy document in AAS. AAS extracted automatable tasks and presents them as depicted in this figure. Detected audit policies are shown on the left. Tasks that need to be performed during the evidence collection and audit for that policy are depicted on the right. Here, the auditor may need to supply additional information that the system cannot automatically provide. This is indicated by the *Edit* symbol. After the audit policy and its tasks have been configured and submitted, the evidence collection and audit is started.

In Figure 46, the auditor is presented an overview of the currently running audit policies, their tasks and configurations as well as associated collection, evaluation and notification agents.

In the examples of Figure 45 and Figure 46, the AAS dashboard had detected the data handling policy with respect to the data retention period. So, for the incident 2 presented in Section 4.5, the auditor can navigate to the result of AAS instance of CardioMon detecting the snapshot created for backup purposes, as shown in Figure 47, in which the violation is presented to the auditor. The particular audit task detected this violation, by collecting evidence from the OpenStack cloud management environment of DataSpacer.

Audit Agent System

Audit overviewCreate auditResultsRecords

# A4Cloud - Audit Agent System

Create audit

Data HandlingAccess controlCustom

Data handling policies

Data retention policy

extract from policy

Tasks

Snapshot check

This audit task checks if a snapshot violation occurred

EditDelete

Configuration

1. Audit type\*Periodic

2. Container\*CMS

3. Check interval:\*320000


4. VM name:\*someCirOSTests

5. Allowed existence time:\*P1Y0M0DT0H0M0S

save

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




Submit

CLOUD  
ACCOUNTABILITY  
PROJECT

A4Cloud Project

www.a4Cloud.eu

Follow us



More side info in the Footer

If you need to present some more information at the bottom, do it here.

1. Maybe in form of a list

2. This footer resizes automatically to fit the contents that you put on it

3. Footers are used mostly to present quick links to information about the service, like to the privacy policy, the contact information, etc.

Disclaimer

Your took might need some kind of disclaimer. If your disclaimer is too long, present the important parts of it here, and provide a link to the full version in a modal dialog, or similar.

Figure 45: Audit Policy Definition from a parsed accountability policy in the AAS instance of CardioMon

FP7-ICT-2011-8-317550-A4CLOUD

Page 65 of 100

Audit Agent System

Audit overviewCreate auditResultsRecords

# A4Cloud - Audit Agent System

## Audit overview

Data HandlingAccess controlCustom

Data handling policies

Data retention policy

Tasks

☐ Snapshot check

This audit task checks if a snapshot violation occurred

Configuration

1. Audit type:

2. Container:

3. OpenStack username:

4. OpenStack password:

5. Endpoint:

6. Port:

7. Tenant:

8. Check interval:

9. VM name:

10. Allowed existence time:

Periodic

CMS

admin

http://localhost

5000

admin

320000

someCirrOSTests

P1Y0M0DT0H0M0S

Running Agents

1. DataRetentionPolicyEvaluationAgent

2. OpenStackRESTAgent

3. EmailNotificationAgent



CLOUD  
ACCOUNTABILITY  
PROJECT

A4Cloud Project

[www.a4cloud.eu](http://www.a4cloud.eu)

Follow us



More side info in the Footer

If you need to present some more information at the bottom, do it here.

1. Maybe in form of a list

2. This footer resizes automatically to fit the contents that you put on it

3. Footers are used mostly to present quick links to information about the service, like to the privacy policy, the contact information, etc.

Disclaimer

Your tool might need some kind of disclaimer. If your disclaimer is too long, present the important parts of it here, and provide a link to the full version in a modal dialog, or similar.

Figure 46: Audit Policy Status and Overview in the CardioMon AAS instance

**Audit Agent System**    Audit overview    Create audit    Results    Records

## A4 Cloud - Audit Agent System

### Results

✖ Violation
⚠ Need review
✔ Passed
Refresh

| Action: snapshot violation  | Policy: data retention policy | Audit task: snapshot check               |
|---|-------------------------------|--|
| This audit task checks if a snapshot violation occurred   |                               |  |
| <b>Evidence</b><br>ActionID: snapshot policy violation@someCirrOSTests<br>ActorID: OpenStackREStAgent@141.28.100.87:1099/JADE<br>Policy reference: 1002<br>Violated rules: a-pl_rule_5<br>Acting tool: OpenStackREStAgent@141.28.100.87:1099/JADE<br>Detection time: 2015-02-17T12:04:02.189<br>Occurance time: N/A |                               |  |
| Action: transfer violation  | Policy: webtraffic policy     | Audit task: apache access log monitoring |

A4Cloud Project  
[www.a4cloud.eu](http://www.a4cloud.eu)  
 Follow us

More side info in the Footer

If you need to present some more information at the bottom, do it here.

- Maybe in form of a list
- This footer resizes automatically to fit the contents that you put on it
- Footers are used mostly to present quick links to information about the service, like to the privacy policy, the contact information, etc.

Disclaimer

Your tool might need some kind of disclaimer. If your disclaimer is too long, present the important parts of it here, and provide a link to the full version in a modal dialog, or similar.

Figure 47: Snapshot violation detection in the CardioMon AAS instance

## 5 Overview of the User Engagement and Evaluation Planning

The user engagement and evaluation plan has been introduced in the WP:D-7 milestone report MS4: Integration and Testing Plan, which was delivered on March 2014. This section builds on top of this document and presents the plan to engage users for validating the A4Cloud concepts through the instantiation of the accountability framework for the wearable use case.

### 5.1 Overview of the Methodology

The plan for user engagement and evaluation is unfold around the user validation methodology, which has been introduced in the milestone report. This methodology has identified the primary evaluation assets, which are summarised in the following lines.

The A4Cloud evaluation methodology sets specific objectives, which aim to bridge the project scientific and technological objectives with the social and ethical dimension of a user validation approach. The scope of the project is to advance the research on *accountability as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services*. By doing so, the project delivers the A4Cloud Accountability Framework, which aims to assist holding



*cloud (and other) service providers accountable for how they manage personal, sensitive and confidential information 'in the cloud'.* The project primary scope is materialised to the following sub-objectives:

- **Objective 1: Support Data Subjects**

Develop tools that enable cloud customers to give their cloud subjects appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.

- **Objective 2: Support Cloud Customers**

Create tools that enable cloud customers to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

- **Objective 3: Support Cloud Providers, Auditors and Supervisory Authorities**

Develop tools to monitor and check compliance with users' expectations, business policies and regulations.

- **Objective 4: Provide the Accountability Handbook**

Develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns, while ensuring that technical mechanisms work to support them.

The main channel for the evaluation of the A4Cloud outcome (the evaluation assets) will be the wearable use case, consisting of the following:

- Presentations explaining the process for the instantiation of the Accountability Framework and tools in the wearable use case.
- The actual use case prototype, operating the wearable service and the A4Cloud tools to provide tangible realisation on the development of the framework in real life scenarios.

As a central point of these assets, we emphasise on the evolution of the Accountability Lifecycle steps from the perspective of each target group from the evaluation audience and the demonstration of the accountability support services.

## **5.2 The dimensions of the evaluation methodology**

For each of the project objectives, the evaluation methodology defines the following evaluation dimensions:

### **i. Capture the user perception on effectiveness**

This dimension enables the understanding of the level of user perception when experiencing with the Accountability Framework and the tools developed to support the various stakeholders in acting on an accountable manner. This evaluation dimension involves the definition of evaluation scenarios, which capture the applicability of the Accountability framework, the relevant mechanisms and tools in various domain specific scenarios and highlight the importance of the framework to facilitate for enhanced data protection mechanism, along with the security and privacy measures adopted by an individual or organisation dealing with the cloud.

### **ii. Monitor the user acceptance**

This dimension aims to build the acceptance profile of the accountability mechanism by collecting valuable feedback from the target stakeholders on the usefulness and effectiveness of the framework and the ICT tools to address multi-stakeholder requirements in the area of accountability and data protection in the cloud. The acceptance profile is built on the strengths and weaknesses of the project outcome, as they are realised by the evaluators, and the opportunities and threats reported and/or discovered during the user validation phase.

### **iii. Investigate on the impact assessment**



In this dimension, the A4Cloud outcome is assessed with respect to being solid enough to offer sustainable solutions for the target markets and stakeholders by elaborating on the exploitation opportunities for the individual accountability tools and the A4Cloud framework itself.

For each of these dimensions, we can define quality metrics, which are used as the basis of the qualitative and quantitative evaluation of the score in each dimension. Saying so, each quality metric is associated with a metric value, which is derived following a certain measurement technique. We consider only those metrics, which can be measured through direct input from the target stakeholders for evaluation, without performing any further processing on their responses. As such, we define the following categories of quality metrics:

- User Perception
  - Completeness of the evaluation assets against the functional requirements
  - Effectiveness of the evaluation assets to address the accountability attributes
  - Capability of the evaluation assets to implement the accountability support services
  - Accuracy of the evaluation assets to deliver the expected artefacts
- User Acceptance
  - Usefulness of the evaluation assets
  - Alignment of the evaluation assets to current business practices
  - Overhead of the evaluation assets for knowledge transfer
  - Increased trust in accomplishing the objectives
- Impact Assessment
  - Benefits brought by the evaluation assets to current business practices
  - Barriers raised by the evaluation assets further wider adoption of the solution framework
  - Coverage of the data protection requirements in current cloud markets
  - Willingness to leverage the use of the Accountability Framework and Tools
  - Overall satisfaction

### 5.3 The Evaluation Audience

Following the project objectives and the target stakeholders for dissemination, as they have been defined in the A4Cloud Deliverable D13.2: Dissemination Plan, we select the appropriate groups of stakeholder representatives in order to perform use validation on the A4Cloud outcome. For the evaluation purposes, we focus on the following groups:

- a) Business and security experts, representing the community of end user organisations, who act as cloud customers;
- b) Individuals, representing the non-ICT skilled end users, who share their data in the cloud;
- c) Cloud providers, representing the cloud service and infrastructure vendors, who conduct their business in cloud;
- d) Auditors and Supervisory Authorities, representing the regulatory community, who define policy frameworks on data protection and are responsible for enforcing cloud service and data protection rules.

It is apparent that, within the context of A4Cloud, it is not feasible to mutually engage in this evaluation process a vast community of people, representing all the potential communities, which have been identified as potential stakeholder groups for dissemination.

## 5.4 The Evaluation Tools

The implementation of the evaluation methodology includes the setup of tools for formalising the stakeholders' feedback in a constructive way. These tools involve the organisation of small scale interviews and focus groups and the availability of questionnaires focused on the needs of the different stakeholder groups from the evaluation audience.

### *The organisation of small scale interviews and focus groups*

Through constructive discussions, these tools are exploited to derive the strong and the strong and weak points of the accountability framework and tools, elaborate on the opportunities and the threats from the adoption of such practices in the current cloud market landscape for protecting the disclosure of personal and business confidential data to third party cloud resources and the implications in the normal operation of cloud-based business scenarios, when checking the compliance of the implemented measures with the local, national and international regulations and legal frameworks.

### *Focused questionnaires*

In order to constructively organise the feedback from the evaluation audience, the use of focused questionnaires is recommended. Such questionnaires will offer the baseline for the collection of the stakeholders' view on the accountability framework, the suggested practices and (mainly the technical) mechanisms. For each evaluation dimension, a set of questions will be used, which aim to reflect the associated quality metrics and collect appropriate qualitative values for them. The questionnaires will be instantiated for each group from the evaluation audience.

## 5.5 Engagement towards evaluation

The engagement to the evaluation process is performed in a two steps approach, namely an intermediate evaluation cycle and a final evaluation period.

### *Intermediate evaluation*

The scope of the intermediate evaluation cycle is to act as an early warning on the work in WP:D-7 in case of considerable deviations from the specifications of the A4Cloud project. As such, the evaluation assets are analysed with respect to the project objectives and the set functional accountability requirements in WP:B-2.

The evaluation audience is selected from all the Consortium partners, based on their profile and expertise in the different research aspects of the development of the Accountability Framework. The selected parties are split into groups, according to their placement in the evaluation audience groups of Section 5.3. Towards this end, ATC is coordinating the process for allocating partners to these groups and organising focused online meetings to interview these parties mainly for the quality metrics on their perception and sustainability potentials. At this point, and since the first prototype of the A4Cloud instantiation to the wearable use case is not provided in full extent, the emphasis should be set on those groups that play a key role in the already supported practices for the preventive and detective accountability mechanisms.

Reaching out of the Consortium, dedicated demonstration events are already in place. A project presentation at the April 2015 Cyber Security and Privacy (CSP) EU Forum is going to be held.

### *Final evaluation*

As we are moving towards the final evaluation, the engagement of various representatives from all the evaluation audience groups is critical. At that point, external to the project stakeholders will be approached to offer their valuable feedback on the supported accountability practices and relevant tools. These parties will be reached through planned dissemination and engagement events. Although the main part of the engagement process will be summarised in the form of discussions, these external stakeholders will be asked to fill in the focused questionnaires in order to provide their value on the quality metrics.

Apart from ad hoc requests for user validation (exploiting the Web Portal as the vehicle to deliver the demonstration process), the project aims to approach key stakeholders for evaluation, through the following two events: a) the organisation of the project Advisory Board Meeting and b) the active participation (through workshops and training) in the November 2015 CSA Congress.

## 6 Conclusions

This document comprises the first deliverable in WP47 describing the instantiation of the A4Cloud outcome in a real business application in the wearables domain. More specifically, D47.1 described the instantiation of the A4Cloud Accountability Framework and the relevant tools to showcase the analysis, development and implementation of the preventive and detective mechanisms for the sake of the wearable use case.

Summarising the contributions of the first prototype for the various target stakeholders of the A4Cloud project, one could say that this prototype showcases how:

- Cloud Customers are guided in making informed choices about how they select cloud service providers that can protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices;
- Cloud Providers are supported in order to define accountability policies and enforce them, while they monitor the normal operation of their cloud services in compliance to their business policies and the established regulatory framework and handle runtime data protection related exceptions on an accountable manner;
- Cloud Auditors and Supervisory Authorities are assisted in performing external verification and compliance checks regarding the use of data by cloud providers and customers, addressing commercial, legal and regulatory obligations, end-user concerns and ensuring that technical mechanisms adopted by these business actors work to support the proper data management procedures.

It must be noted that in order to validate the proper deployment of the A4Cloud tools for the wearable use case, we performed a list of functional tests to experiment with the integration and configuration of these tools. According to the A4Cloud Description of Work, this task is attributed to the work performed in WP:46 and it will be reported in the relevant deliverables of this WP.

Following this version of the prototype, the project aims for an intermediate user validation of the application of the A4Cloud framework and tools in the wearable use case. The results of this validation phase will join up with the work planned for the final prototype. In order to better manage the integration work, as well as to progressively assess the impact of the implementation of A4Cloud mechanisms in the wearable use case, this last phase will be delivered gradually in two steps, which are identified through the delivery of an intermediate and a final A4Cloud prototype.

- The intermediate prototype will be delivered by M33 (end of June 2015) and will include:
- An initial version of the semi-automatic approach for policy definition;
- An enhanced version of the policy enforcement face, facilitating integration with the evidence collection and incident response parts;
- A draft implementation of the semi-automatic approach for the deployment of accountability measures through AT;
- An integrated approach for the evidence store hosted by cloud providers;
- The data subject enablement part;
- A draft development of the tools implementing the corrective accountability mechanisms;

The final instantiation of the A4Cloud accountability framework and the respective tools is planned for M36.

## 7 References

- [1] A4Cloud, Deliverable D32.1: "D:C-2.1 Report detailing conceptual framework", October 2014.
- [2] A4Cloud, Deliverable D23.2: "D:B-3.2 Consolidated Use Case Report", September 2014.
- [3] A4Cloud Deliverable D33.1: "D:C-3.1 Requirements for cloud interoperability", November 2013.

- [4] A4Cloud, Deliverable D42.3: "D:D-2.3 Initial Reference Architecture", March 2015.
- [5] A4Cloud, Deliverable D43.2: "D:D-3.2 Prototype for accountability enforcement tools and services", March 2015
- [6] OpenStack, <https://www.openstack.org/>.
- [7] OpenStack Icehouse, <http://www.openstack.org/software/icehouse/>.
- [8] OpenStack Icehouse, Installation Guidelines – Architecture, [http://docs.openstack.org/icehouse/install-guide/install/apt/content/ch\\_overview.html](http://docs.openstack.org/icehouse/install-guide/install/apt/content/ch_overview.html)
- [9] Ubuntu, <http://www.ubuntu.com/>.
- [10] Apache HTTP Server Project, <http://httpd.apache.org/download.cgi>
- [11] Apache Tomcat, <http://tomcat.apache.org/>
- [12] The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Group Note 13 November 2006, <http://www.w3.org/TR/P3P11/>
- [13] eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard, 22 January 2013
- [14] PuTTY: A Free Telnet/SSH Client, <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- [15] DTMT Readme file, December 2014
- [16] A4Cloud Deliverable D38.3 "Automation Service for the Framework of Evidence", March 2015

## 8 Appendices

### 8.1 Aspects of the Use Case Development

In order to connect the Wearable Service business application logic with the A4Cloud tools and especially with the A-PPLE instance of CardioMon, an intermediate service layer has been implemented, which serves the UI functionalities of Table 1, based on the API methods offered by A-PPLE. Thus, this section describes these REST Web services by providing their API format and their link to the relevant UI screen(s).

#### 8.1.1 Registration Service

Upon registration, first invoke the *Trigger Registration Service*:

|                         |   |
|-------------------------|---|
| <b>Description</b>      | The user is presented with the human readable policy that has to be accepted in order for the user to be able to register to the Wearable Service |
| <b>Linked to Screen</b> | Screen 1  |
| <b>API method type</b>  | GET   |
| <b>End point</b>        | ../appl-help/rest/triggerRegistration   |
| <b>Example Input</b>    | -   |
| <b>Example Output</b>   | {status: OK/404}  |

Then, invoke the *Fill in Registration Form* service:

|                         |  |
|-------------------------|--|
| <b>Description</b>      | The user provides the data to fill in the wellbeing profile upon registering to the Wearable Service   |
| <b>Linked to Screen</b> | Screen 2   |
| <b>API method type</b>  | POST   |
| <b>End point</b>        | ../appl-help/rest/register   |
| <b>Example Input</b>    | {       "username": "gio",       "password": "pass",       "displayName": "giopnd",       "gender": "male",       "country": "Italy",       "dateOfBirth": 1,       "height": 2,       "weight": 3,       "email": "g.giotis@atc.gr",       "pathToPolicy": "/policy1.xml"     } |
| <b>Example Output</b>   | {status: OK}   |

### 8.1.2 Update PII

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Update the specific PII of a given owner. Assuming request having been sent by an authenticated data subject  |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | POST  |
| <b>End point</b>        | ../appl-help/rest/updatePii   |
| <b>Example Input</b>    | {       "subject": "Data Subject",       "purpose": "health",       "action": "update",       "resourceName": "sugar level",       "newValue": "100",       "owner": "gio",       "date": null,       "authorization": ""     } |
| <b>Example Output</b>   | -   |

Note: Use always “Data Subject” as subject, except for Map-On-Web statistics. Purpose should always be “health”.

### 8.1.3 Request Real-time information: Histogram Visualisation

|                         |  |
|-------------------------|--|
| <b>Description</b>      | Get the distribution of the daily average wellbeing statistics for specific resource, user and month.  |
| <b>Linked to Screen</b> |  |
| <b>API method type</b>  | POST   |
| <b>End point</b>        | ../appl-help/rest/getPiiHistoryOwner   |
| <b>Example Input</b>    | {       "subject": "Data Subject",       "purpose": "health",       "action": "read",       "resourceName": "sugar level",       "owner": "gio",       "authorization": ""     } |

|                       |                                |
|-----------------------|--------------------------------|
|                       | "date": "2015-03-30 14:29:40"} |
| <b>Example Output</b> | {"30":220.0,"29":100.0}        |

Notes: Use always “Data Subject” as subject, except for Map-On-Web statistics. Purpose should always be “health”. In the response, formatted in JSON, each attribute name corresponds to a day index in the provided month.

#### 8.1.4 Request Real-time information: Average Values

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Get average wellbeing statistics for specific user aggregated by resource.  |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | POST  |
| <b>End point</b>        | ../appl-help/rest/getPiiAvgHistoryOwner   |
| <b>Example Input</b>    | {"subject": "Data Subject",<br>"purpose": "health",<br>"action": "read",<br>"owner": "gio",<br>"authorization": ""} |
| <b>Example Output</b>   | {"heartbeat rate":0.0,"sugar level":160.0,"blood pressure":0.0}   |

Notes: Use always “Data Subject” as subject, except for Map-On-Web statistics. Purpose should always be “health”. Predefined thresholds have been used to calculate average percentage values.

#### 8.1.5 View activities: Wellbeing statistics

|                         |  |
|-------------------------|--|
| <b>Description</b>      | Get average wellbeing statistics for specific user and date aggregated by resource.  |
| <b>Linked to Screen</b> |  |
| <b>API method type</b>  | POST   |
| <b>End point</b>        | ../appl-help/rest/getPiiAvgHistoryOwnerOnDate  |
| <b>Example Input</b>    | {"subject": "Data Subject",<br>"purpose": "health",<br>"action": "read",<br>"owner": "gio",<br>"authorization": "",<br>"date": "2015-03-30"} |
| <b>Example Output</b>   | {"heartbeat rate":40.0,"sugar level":220.0,"blood pressure":0.0}   |

#### 8.1.6 View activities: Get activities on date

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Get the wellbeing activities for specific user and date aggregated by resource. |
| <b>Linked to Screen</b> |   |

|                        |   |
|------------------------|---|
| <b>API method type</b> | POST  |
| <b>End point</b>       | ../appl-help/rest/getActivitiesByOwnerOnDate  |
| <b>Example Input</b>   | {<br>"subject": "Data Subject",<br>"purpose": "health",<br>"action": "read",<br>"owner": "gio",<br>"authorization": "",<br>"date": "2015-03-30"}<br>} |
| <b>Example Output</b>  | [{"workout": {}}, {"yoga": {"time": "2015-03-30 16:45:09.0", "value": "41"}}, {"swimming": {}}, {"running": {}}]                                      |

### 8.1.7 Active users

First, invoke the *allOwners* service:

|                         |  |
|-------------------------|--|
| <b>Description</b>      | Get all 'username' PII's.  |
| <b>Linked to Screen</b> |  |
| <b>API method type</b>  | GET  |
| <b>End point</b>        | ../apple-rest/pii/allOwners?subject=Employee&resourceName=username&purpose=http://www.w3.org/2002/01/P3Pv1/health&action=read&authorization= |
| <b>Example Input</b>    | -  |
| <b>Example Output</b>   | ["gio", "mike"]  |

Then, for each username (which corresponds to each owner), get the resource you need to display, through the A-PPLE Rest API method:

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Request resource of specific owner for specific purpose and action.   |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | GET   |
| <b>End point</b>        | ../apple-rest/pii?subject=Employee&resourceName=country&owner=gio&purpose=http://www.w3.org/2002/01/P3Pv1/health&action=read&authorization= |
| <b>Example Input</b>    | -   |
| <b>Example Output</b>   | {<br>id: 5<br>name: "country"<br>value: "Italy"<br>creationDate: "2015-03-31 13:24:48.414"<br>modificationDate: null<br>}                   |

If method invoker is not authorised to access specific resource, a "401 Unauthorized" message is received.



## 8.1.8 Statistics

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Get average wellbeing statistics for all users aggregated by resource.                          |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | POST  |
| <b>End point</b>        | ../appl-help/rest/getPiiHistoryAll  |
| <b>Example Input</b>    | { "subject": "Map-On-Web",<br>"purpose": "health",<br>"action": "read",<br>"authorization": ""} |
| <b>Example Output</b>   | [{"blood pressure":75.0}, {"heartbeat rate": 15.0},<br>{"sugar level": 915.0}]                  |

## 8.1.9 Map Visualisation

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Get average wellbeing statistics for all users and for specific resource aggregated by country.                                   |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | POST  |
| <b>End point</b>        | ../appl-help/rest/getPiiHistoryAllGroupByCountry  |
| <b>Example Input</b>    | { "subject": "Map-On-Web",<br>"purpose": "health",<br>"action": "read",<br>"resourceName": "sugar level",<br>"authorization": ""} |
| <b>Example Output</b>   | [{"hc-key":"ee", "value":100.0}, {"hc-key":"Greece", "value":1216.6666666666667}, {"hc-key":"Italy", "value":60.0}]               |

## 8.1.10 Alert messages

|                         |  |
|-------------------------|--|
| <b>Description</b>      | Get policy violations regarding 'Access denied' and 'DTMT' events.   |
| <b>Linked to Screen</b> |  |
| <b>API method type</b>  | GET  |
| <b>End point</b>        | ../appl-help/rest/getPolicyViolations  |
| <b>Example Input</b>    | -  |
| <b>Example Output</b>   | [{"message":"Event associated with personal data 'heartbeat rate' belonging to 'bill', access attempt by subject 'Employee': Access denied for, for action 'read'", "owner":"bill", "date":"2015-04-02 14:19:49.0"}] |

## 8.1.11 Get PII all

|                         |                                  |
|-------------------------|----------------------------------|
| <b>Description</b>      | Get all PIIs of a specific owner |
| <b>Linked to Screen</b> |                                  |

|                        |  |
|------------------------|--|
| <b>API method type</b> | GET  |
| <b>End point</b>       | ../apple-rest/pii/all?subject=gio&owner=gio&authorization=   |
| <b>Example Input</b>   | -  |
| <b>Example Output</b>  | <pre>{   "allPii": [     {       "id": 1,       "name": "username",       "value": "gio",       "creationDate": "2015-04-02 11:27:45.0",       "modificationDate": null     },     {       "id": 2,       "name": "password",       "value": "pass",       "creationDate": "2015-04-02 11:27:53.0",       "modificationDate": null     },     {       "id": 3,       "name": "display name",       "value": "giopnd",       "creationDate": "2015-04-02 11:27:58.0",       "modificationDate": null     },     {       "id": 4,       "name": "gender",       "value": "male",       "creationDate": "2015-04-02 11:28:03.0",       "modificationDate": null     },     {       "id": 5,       "name": "country",       "value": "mc",       "creationDate": "2015-04-02 11:28:08.0",       "modificationDate": null     },     {       "id": 6,       "name": "date of birth",       "value": "1",       "creationDate": "2015-04-02 11:28:13.0",       "modificationDate": null     },     {       "id": 7,       "name": "height",       "value": "2.0",       "creationDate": "2015-04-02 11:28:17.0",       "modificationDate": null     },     {       "id": 8,       "name": "weight",       "value": "3.0",       "creationDate": "2015-04-02 11:28:23.0",       "modificationDate": null     },     {       "id": 9,       "name": "email",       "value": "g.giotis@atc.gr",       "creationDate": "2015-04-02 11:28:28.0",       "modificationDate": null     },     {       "id": 10,       "name": "sugar level",       "value": "60",       "creationDate": "2015-04-02 11:28:33.0",       "modificationDate": "2015-04-02 11:39:28.0"     },     {       "id": 11,       "name": "blood pressure",       "value": "111",       "creationDate": "2015-04-02 11:28:38.0",       "modificationDate": "2015-04-02 11:41:32.0"     },     {       "id": 12,       "name": "heartbeat rate",       "value": "340",       "creationDate": "2015-04-02 11:28:43.0",       "modificationDate": "2015-04-02 11:39:46.0"     },     {       "id": 13,       "name": "workout",       "value": "0",       "creationDate": "2015-04-02 11:28:48.0",       "modificationDate": null     },     {       "id": 14,       "name": "yoga",       "value": "0",       "creationDate": "2015-04-02 11:28:54.0",       "modificationDate": null     },     {       "id": 15,       "name": "swimming",       "value": "0",       "creationDate": "2015-04-02 11:28:59.0",       "modificationDate": null     },     {       "id": 16,       "name": "running",       "value": "0",       "creationDate": "2015-04-02 11:29:04.0",       "modificationDate": null     }   ] }</pre> |

Notes: Subject should always be the same as owner.

#### 8.1.12 Delete PII all

|                         |   |
|-------------------------|---|
| <b>Description</b>      | Delete all PII of a given owner from database. Assuming request having been sent by an authenticated data subject. Only the data subject should use this functionality. |
| <b>Linked to Screen</b> |   |
| <b>API method type</b>  | DELETE  |
| <b>End point</b>        | ../apple-rest/pii/all?subject=bill&owner=bill&authorization=  |

|                       |                  |
|-----------------------|------------------|
| <b>Example Input</b>  | -                |
| <b>Example Output</b> | {"deleted":true} |

Note: Requesting subject should always be the owner.

## 8.2 The high level legal and normative obligations of the use case roles

This section lists the high level legal and normative obligations of the use case actors, according to their assigned role in the use case demonstration. The relevant tables are not limited only to the obligations being demonstrated in this first prototype.

DataSpacer is a cloud IaaS provider, which acts as a data processor for both the Map-on-Web and CardioMon. This provider should accept responsibility on the legal and normative obligations shown in Table 7.

Table 7: The legal and normative obligations of DataSpacer

| Obligation reference                           | Description of the obligations for DataSpacer   |
|--|---|
| <i>From Legal Perspective</i>                  |   |
| DS1: informing about the use of sub-processors | DataSpacer is accountable to all of its customers that provide personal data (including Map-on-Web and CardioMon) for informing about the use of sub-providers to process these data                        |
| DS2: evidence of data processing               | DataSpacer is accountable to all of its customers that provide personal data (including Map-on-Web and CardioMon) for, upon request, providing evidence on their data processing practices                  |
| DS3: evidence of data deletion                 | DataSpacer is accountable to all of its customers that provide personal data (including Map-on-Web and CardioMon) for, upon request, providing evidence on the correct and timely deletion of personal data |
| <i>From Normative Perspective</i>              |   |
| Obligation: privacy-by-default                 | By default, DataSpacer implements the strongest privacy settings as the default ones, when receiving personal data for storage  |
| Obligation: monitoring of data practices       | DataSpacer should monitor their actual data practices and keep records of the monitoring and its results  |
| Obligation: compliance with privacy policies   | DataSpacer should be able to demonstrate to any customer (including Map-on-Web and CardioMon) compliance with their policies in a timely fashion “reactively” and where possible “proactively”.             |
| Obligation: informing about policy violations  | DataSpacer should be able to inform their customers (including Map-on-Web and CardioMon) about any policy violations that are related to any personal data processed within their range of authority        |
| Obligation: remediation in case of damages     | DataSpacer should be able to provide remediation to their customers (including Map-on-Web and CardioMon) in the case of damages caused to data subjects due to processing of personal data                  |

CardioMon is a cloud SaaS provider, acting as a data processor and operating the Wearable Service on behalf of the Wearable Co. This provider should accept responsibility on the legal and normative obligations shown in Table 8.

Table 8: The legal and normative obligations of CardioMon

| Obligation Reference                                       | Description of the Obligations for CardioMon  |
|--|---|
| <i>From Legal Perspective</i>                              |   |
| C1: informing about the use of sub-processors              | CardioMon is accountable to any collaborating party (including the Wearable Co) for informing about the use of DataSpacer to process personal data  |
| C2: evidence of data processing                            | CardioMon is accountable to any collaborating party (including the Wearable Co) for, upon request, providing evidence on their data processing practices  |
| C3: evidence of data deletion                              | CardioMon is accountable to any collaborating party (including the Wearable Co) for, upon request, providing evidence on the correct and timely deletion of personal data   |
| <i>From Normative Perspective</i>                          |   |
| Obligation: privacy-by-default                             | By default, CardioMon implements the strongest privacy settings as the default ones, when receiving personal data for processing  |
| Obligation: specifying user preferences                    | CardioMon should offer their customers (including the Wearable Co) services that allow the users (the wearable customers for the Wearable use case) to specify privacy preferences, for example with respect to how their data are used by the Map-on-Web |
| Obligation: monitoring of data practices                   | CardioMon should monitor their actual data practices and keep records of the monitoring and its results   |
| Obligation: compliance with privacy policies               | CardioMon should be able to demonstrate to any customer (including the Wearable Co) compliance with their policies in a timely fashion “reactively” and where possible “proactively”  |
| Obligation: compliance with user preferences               | CardioMon should be able to provide evidences to their customers (including the Wearable Co) that personal data is processed in accordance to their preferences   |
| Obligation: informing about policy violations              | CardioMon should be able to inform their customers (including the Wearable Co) about any policy violations that are related to any personal data processed within their range of authority  |
| Obligation: informing about privacy preferences violations | CardioMon should inform their customers (including the Wearable Co) and their users (the wearable customers in the Wearable use case) about any violations of their privacy preferences   |
| Obligation: remediation in case of damages                 | CardioMon should be able to provide remediation to their customers (including the Wearable Co) in the case of damages caused to data subjects (the wearable customers in the Wearable use case) due to processing of personal data                        |

The Wearable Co is a cloud customer, acting as a data controller determining on which data of the wearable customers should be collected and processed during the operation of the Wearable Service. This customer should accept responsibility on the legal and normative obligations shown in Table 9.

Table 9: The legal and normative obligations of Wearable Co

| Obligation Reference                                      | Description of the Obligations for Wearable Co   |
|---|--|
| <i>From a Legal Perspective</i>                           |  |
| W1: informing about processing                            | Wearable Co is accountable to the wearable customers for informing that their personal data are being collected and processed by CardioMon   |
| W2: informing about purpose                               | Wearable Co is accountable to the wearable customers for informing about the purpose of collecting and processing their personal data  |
| W3: informing about recipients                            | Wearable Co is accountable to the wearable customers for informing about the recipients (CardioMon) of their personal data   |
| W4: informing about rights                                | Wearable Co is accountable to the wearable customers for informing about the existence of their rights to access and rectify the collected personal data   |
| W5: data collection purposes                              | Wearable Co is accountable to the wearable customers for collecting personal data only for specific, explicit and legitimate purposes. Moreover, the Wearable Co is accountable to the wearable customers for processing their personal data only for the stated purposes. |
| W6: the right to access, correct and delete personal data | Wearable Co is accountable to the wearable customers for making it possible for them to access, collect and rectify their personal data  |
| W7: data storage period                                   | Wearable Co is accountable to the wearable customers for keeping their personal data in a form which permits identification for no longer than necessary   |
| W8: security and privacy measures                         | Wearable Co is accountable to the wearable customers for the security and privacy of the personal data they collect  |
| W9: rules for data processing by provider                 | Wearable Co is accountable to the wearable customers for how CardioMon processes the wearable customers' personal data.  |
| W10: rules for data processing by sub-provider            | Wearable Co is accountable to the wearable customers for how DataSpacer and Map-on-Web (engaged as sub-providers to CardioMon) process the customers' personal data  |
| W11: provider safeguards                                  | Wearable Co is accountable to the wearable customers for choosing cloud providers (CardioMon in the Wearable use case) that can provide sufficient safeguards concerning technical security and organisational measures  |
| W12: sub-provider safeguards                              | Wearable Co is accountable to the wearable customers for ensuring that all sub-providers involved in the service delivery chain (that is DataSpacer and Map-on-Web) provide sufficient safeguards to protect the personal data that they process                           |
| W13: informed consent to processing                       | Wearable Co is accountable to the wearable customers for obtaining informed consent before collecting their personal data  |
| W14: explicit consent to processing                       | Wearable Co is accountable to the wearable customers for obtaining their explicit consent before collecting any sensitive personal data  |

| Obligation Reference                                 | Description of the Obligations for Wearable Co  |
|--|---|
| W15: informing DPAs                                  | Wearable Co is accountable to the Greek Data Protection Authority to inform that they collect personal data   |
| W16: security breach notification                    | Wearable Co is accountable to the wearable customers for notifying them of security incidents that are related to their personal data                                 |
| W17: data location                                   | Wearable Co is accountable to the wearable customers for informing them about the location of the processing of their personal data (Europe in the Wearable use case) |
| <i>From a Normative Perspective</i>                  |   |
| Obligation: informing about personal data processing | Wearable Co should inform CardioMon that they will use their services to process personal data  |

### 8.3 The Lawyer Readable Privacy Policy

16th of March 2015

#### Privacy Policy of Wearable Company<sup>7</sup>

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:

- (a) administer our Wearable Service;
- (b) personalise our Wearable Service for you;
- (c) enable your use of the functionalities available on our Wearable Service for monitoring and updating your personal information collected from your wearable device or provided by you through this service;
- (d) send you statistical information about the personal information collected from all of our customers through our Wearable Service;
- (e) send you notifications and alerts on excessive wellbeing values, according to your profile, and any other violation on this policy or any security breach;
- (f) personal information will be used to produce statistical information, which will be compiled by third parties;

<sup>7</sup> +Spaces Project, Deliverable D7.4 Legal Evaluation Report, available at [http://ec.europa.eu/information\\_society/apps/projects/logos/6/248726/080/deliverables/001\\_SpacesD74V10.pdf](http://ec.europa.eu/information_society/apps/projects/logos/6/248726/080/deliverables/001_SpacesD74V10.pdf) and Privacy policy of Withings Company available at [http://www-media-cdn.withings.com/wysiwyg/legal/2015-Privacy-Policy-VEE.pdf?\\_ga=1.4133936.1418836187.1421433226](http://www-media-cdn.withings.com/wysiwyg/legal/2015-Privacy-Policy-VEE.pdf?_ga=1.4133936.1418836187.1421433226).

(g) verify compliance with the terms and conditions governing the use of our Wearable Service;

Your data will not be used for any other purposes than those listed above. Your data will not be used for direct marketing purposes.

Wearable company stores the data collected only for as long as it is necessary for the delivery of the services offered through Wearable devices. Apart from where the law stipulates a specific period, we retain your personal data for a period not exceeding the period required for the purposes for which it was collected and processed. We therefore retain your personal data attached to your account until the account deletion.

In compliance to our legal obligations with respect to the retention and deletion of personal information, we set out specific conditions for our data retention policies and procedure.

Any personal information processed by the Wearable Service for the purposes stated in this policy shall not be kept for longer than is necessary for those purposes.

We will usually delete any personal data applicable in this policy being more than 6 months old. We will usually delete any personal data applicable in this policy, if your request deletion of your account to our Wearable Service. Notwithstanding the other provisions of this Section, we will retain documents (including electronic documents) containing personal data:

- (a) to the extent that we are required to do so by law;
- (b) if we believe that the documents may be relevant to any ongoing or prospective legal proceedings; and
- (c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);

#### About the data that will be processed

Wearable Application processes data collected through the Wearable devices. Those data identify you either directly or indirectly. Data that identifies you directly may be your first name or surname, your date of birth, your e-mail address, your photo, etc. We may also collect data that identify you indirectly such as your weight, your postcode, etc.

In particular, Wearable devices collect the following types of data:

- (a) information about your wearable device and about the information for you recorded from this device per time unit (including the Sugar Level, the Blood Pressure and Heartbeat Rate);
- (b) information that you provide to us when registering with our Wearable Service (including your Username and Password);
- (c) information that you provide when completing your profile on our Wearable Service (including your Display Name, Gender, Age, Height, Weight and Country of origin);
- (d) information that you provide to us when using the service on our Wearable Service, or that is generated in the course of the use of those services (including your daily wellbeing activities); and
- (e) any other personal information that you choose to send to us (eg when filling in the optional field of the account form)

Note that Wearable devices use cookies. A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server. If you block cookies, you will not be able to use all the features on our Wearable Service.

#### About your rights

You can have access to your personal data. Wearable Company keep your data in an open format for you to easily keep and access them.

You can amend your personal information at any time, add to, delete or update the personal data produced by an active measurement on your part. This may be done directly in the application or on request. Upon your request to delete your profile, all your personal information will be deleted within 6 months.



You can object to your data being processed by contacting our customer service department. You may object for legitimate reasons to your data being processed. However, you should be aware that this action might limit the scope of Wearable Application and devices.

To protect your privacy and the privacy of others, we may have to verify that you are who you are before we can give you access to, or change, information about you.

#### Access to personal information by third parties

Wearable Application will be hosted by the servers of CardioMon, located in Athens. CardioMon is a primary service provider, acting as a data processor. CardioMon will process information on behalf and upon further instructions of the data controller, the Wearable Company.

CardioMon has access to your personal information for the purposes arising from the functionalities available on our Wearable Service and as they are set out in this policy. CardioMon may disclose further personal information to its subcontractor Map-on-Web, only when and if this is required for the purposes set out in this policy.

Wearable company uses certain trusted third parties to help us provide, improve, protect, and promote our Services. These third parties will access your information only to perform tasks on our behalf and in compliance with this Privacy Policy. Our Wearable Service includes the visualisation of the statistical information about the personal information collected from all of our customers provided by third party applications.

We ensure that your personal data will not be disclosed to state institutions and Law Enforcement authorities, except if required by law.

#### Security measures

Wearable company shall take the appropriate technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

You are responsible for keeping the password you use for accessing our Wearable Service confidential;

#### Data transfers to international data centres

Personal information that we collect from you may be stored and processed in and transferred between any of the countries in which we operate within the EEA in order to enable us to use the information in accordance with this policy.

Any other transfer of personal data outside of EEA is forbidden.

We may change our privacy policy to adapt to your needs, to the evolution of the legal framework or when we develop our products and services. We shall inform you of any modification performed well in advance.

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

```

```

database -->
    <!-- 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 duration="P0Y0M0DT00H10M0S"
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>
```

## 8.5 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
    ID</xacml:AttributeValue>
                            Machine
```

```

                                <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 Index of figures

|  |    |
|--|----|
| Figure 1: The conceptualisation of the Wearable Service.....   | 9  |
| Figure 2: The use case overview for the Wearable Service – the Business Perspective .....  | 11 |
| Figure 3: The functional elements of the Accountability Lifecycle.....   | 16 |
| Figure 4: The perspective of the Wearable Use Case for the implementation of preventive accountability mechanisms .....            | 17 |
| Figure 5: The perspective of the Wearable Use Case for the implementation of the detective accountability mechanisms.....          | 19 |
| Figure 6: The perspective of the Wearable Use Case for the implementation of the corrective accountability mechanisms.....         | 20 |
| Figure 7: The deployment of the A4Cloud tools in DataSpacer .....  | 24 |
| Figure 8: The deployment of the A4Cloud tools for the collaboration of DataSpacer with Map-on-Web .....                            | 25 |
| Figure 9: The physical deployment of the A4Cloud tools for the complete cloud service supply chain of the wearable use case.....   | 26 |
| Figure 10: The process of the Wearable Co to use COAT in order to select CardioMon .....   | 27 |
| Figure 11: The process of the Wearable Co to use COAT in order to select CardioMon .....   | 28 |
| Figure 12: The alternative flows for the generation of the machine readable accountability policies ...                            | 29 |
| Figure 13: The process for the enforcement of the policy rules in the various actors of the wearable use case .....                | 32 |
| Figure 14: An example process for the collection and management of evidence in case of a data access incident .....                | 33 |
| Figure 15: An example process for the collection and management of evidence in case of a data retention incident .....             | 34 |
| Figure 16: An example process for the collection and management of evidence in case of a data transfer incident .....              | 35 |
| Figure 17: The implementation of the data subject enablement process .....   | 36 |
| Figure 18: The process for the implementation of the notification accountability support services of corrective mechanisms.....    | 37 |
| Figure 19: The process for the implementation of the remediation accountability support services of the corrective mechanisms..... | 38 |
| Figure 20: CardioMon Privacy Officer using COAT to select the target service type .....  | 41 |
| Figure 21: CardioMon Privacy Officer using COAT to select requirements.....  | 42 |
| Figure 22: CardioMon Privacy Officer inspecting the details of the DataSpacer contract .....                                       | 43 |
| Figure 23: DPIAT Landing Page .....  | 44 |
| Figure 24: Report page of the Pre-screening questionnaire .....  | 44 |
| Figure 25: Example view of the screening questionnaire taken by the Privacy Officer of CardioMon..                                 | 45 |
| Figure 26: Example DPIAT report for the risk assessment on DataSpacer .....  | 46 |
| Figure 27: The architecture of the Wearable Service for the Wearable Co .....  | 51 |
| Figure 28: The home page of the Wearable Service .....   | 53 |
| Figure 29: The login page of the Wearable Service .....  | 54 |

|   |    |
|---|----|
| Figure 30: The consent form that the wearable customer needs to accept during the registration phase .....                          | 54 |
| Figure 31: The Registration page of the Wearable Service .....  | 55 |
| Figure 32: The first page of the logged in Wearable Customers.....  | 56 |
| Figure 33: The real time information page of the logged in Wearable Customers.....  | 56 |
| Figure 34: The Wearable Service page for chart visualisation of the real time information for the logged in Wearable Customers..... | 57 |
| Figure 35: The screen of the Wearable Service to manage wellbeing activities.....   | 57 |
| Figure 36: Managing activities in the wearable Service .....  | 58 |
| Figure 37: The Manage Profile page of the Wearable Service .....  | 59 |
| Figure 38: The statistical Map visualisation page of the Wearable Service .....   | 59 |
| Figure 39: The first page of the logged in Employees.....   | 60 |
| Figure 40: An employee viewing the profile of a wearable customer.....  | 60 |
| Figure 41: The alerts page of the Wearable Service.....   | 61 |
| Figure 42: Creating a snapshot of the CardioMon VM through the OpenStack dashboard .....  | 62 |
| Figure 43: Attach-detach a data volume from a compute node .....  | 63 |
| Figure 44: CardioMon AAS Dashboard Overview.....  | 64 |
| Figure 45: Audit Policy Definition from a parsed accountability policy in the AAS instance of CardioMon .....                       | 65 |
| Figure 46: Audit Policy Status and Overview in the CardioMon AAS instance.....  | 66 |
| Figure 47: Snapshot violation detection in the CardioMon AAS instance.....  | 67 |

## 10 Index of tables

|  |    |
|--|----|
| Table 1: The user level functionalities of the Wearable Service .....  | 12 |
| Table 2: Type of data comprising the wellbeing profile .....   | 13 |
| Table 3: The assignment of roles to the actors of the Wearable Service Use Case.....   | 14 |
| Table 4: The incident types considered in the specification of the Wearable Use Case .....                                   | 18 |
| Table 5: The first instantiation of the A4Cloud Cloud Accountability Reference Architecture for the wearable use case.....   | 22 |
| Table 6: The Wearable Service UI level functionalities of the wearable customer and accountability related requirements..... | 46 |
| Table 7: The legal and normative obligations of DataSpacer .....   | 78 |
| Table 8: The legal and normative obligations of CardioMon.....   | 79 |
| Table 9: The legal and normative obligations of Wearable Co .....  | 80 |