The research leading to these results has received funding from the European Community’s H2020 research and innovation programme under grant agreement n° 731678.
<table>
<thead>
<tr>
<th>Project Number</th>
<th>731678</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Title</td>
<td>RestAssured - Secure Data Processing in the Cloud</td>
</tr>
<tr>
<td>Deliverable Type</td>
<td>External Report</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title of Deliverable</th>
<th>D8.1 - First Validation Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nature of Deliverable</td>
<td>External Report</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Contractual Delivery Date</td>
<td>31 July 2017</td>
</tr>
<tr>
<td>Actual Delivery Date</td>
<td>31 July 2017</td>
</tr>
<tr>
<td>Contributing WPs</td>
<td>All</td>
</tr>
<tr>
<td>Editor(s)</td>
<td>Paul Mundt, Adam Burns</td>
</tr>
</tbody>
</table>
# Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul Mundt</td>
<td>Adaptant</td>
<td>Sections 1-4</td>
</tr>
<tr>
<td>Adam Burns</td>
<td>Adaptant</td>
<td>Sections 1-4</td>
</tr>
<tr>
<td>Will Saunders</td>
<td>OCC</td>
<td>Section 3</td>
</tr>
</tbody>
</table>
### Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>06.06.2017</td>
<td>Initial draft</td>
</tr>
<tr>
<td>V0.5</td>
<td>15.07.2017</td>
<td>Draft incorporating comments from Brussels face to face meeting</td>
</tr>
<tr>
<td>V0.6</td>
<td>22.07.2017</td>
<td>Pre-Internal Review Draft</td>
</tr>
<tr>
<td>V0.7</td>
<td>22.07.2017</td>
<td>Internal Review Draft</td>
</tr>
<tr>
<td>V0.7.2</td>
<td>25.07.2017</td>
<td>External Review Draft</td>
</tr>
<tr>
<td>V0.8</td>
<td>28.07.2017</td>
<td>Final Review Draft</td>
</tr>
<tr>
<td>V1.0</td>
<td>30.07.2017</td>
<td>Version submitted to EC</td>
</tr>
</tbody>
</table>
## Contents

**List of Figures** ........................................................................ 7

1 **Introduction** ...................................................................... 8
  1.1 **Purpose** .................................................................. 8
  1.2 **RestAssured Components** ........................................... 9
    1.2.1 Orchestration of the RestAssured Components .............. 9
  1.3 **RestAssured Application Microservice Pipeline Reference Examples** ........................................ 10
    1.3.1 Web and REST API Pipeline Reference Example ........... 10
    1.3.2 Data Stream Pipeline Reference Example .................. 11
    1.3.3 RestAssured Applications and Multiple Microservice Pipelines ............................................. 11

2 **Pay as You Drive: Usage Based Automobile Insurance** ............. 12
  2.1 **Introduction** .......................................................... 12
  2.2 **State of the Art** ....................................................... 12
    2.2.1 Introduction to Usage Based Insurance Models ......... 12
    2.2.2 Connected Cars .................................................... 13
    2.2.3 Telematics Service Providers .................................. 13
  2.3 **Gap Analysis** .......................................................... 15
    2.3.1 Current Environment .............................................. 15
    2.3.2 RestAssured Solution Overview ............................... 17
  2.4 **Stakeholder Definitions and Stories** ................................. 19
    2.4.1 Driver ................................................................. 19
    2.4.2 Insurance Service Provider ...................................... 19
    2.4.3 Telematics Provider ............................................... 20
    2.4.4 Insurer and Telematics Infrastructure as a Service (IaaS) Providers ........................................... 20
    2.4.5 Insurer and Telematics Platform as a Service (PaaS) Providers .................................................. 20
  2.5 **Validation Environment Overview** .................................. 21
  2.6 **Validation Scenarios** .................................................. 21
    2.6.1 Driver grants consent for Telematics Provider access to telematic data ....................................... 22
    2.6.2 Driver withdraws consent for Telematics Provider access to telematic data ................................. 22
    2.6.3 Driver grants consent for Telematics Provider for aggregate use .............................................. 23
    2.6.4 Driver grants consent for Telematics Provider for anonymous use ............................................ 24
  2.7 **Validation Conclusions** ............................................... 24
3 CARE: Self Directed Social Care

3.1 Introduction

3.2 State of the Art

3.2.1 Introduction to Self-Directed Social Care (Ami)

3.3 Gap Analysis

3.3.1 Current Environment

3.3.2 RestAssured Solution Overview

3.4 Stakeholder Definitions and Stories

3.4.1 Volunteer

3.4.2 Client

3.4.3 Third Party Volunteer Organisation

3.4.4 Local Authority

3.4.5 Service Provider

3.4.6 Infrastructure as a Service (IaaS) Provider

3.4.7 Platform as a Service (PaaS) Provider

3.5 Validation Environment Overview

3.6 Validation Scenarios

3.6.1 Volunteer grants consent for third party access to anonymised personal data

3.6.2 Volunteer withdraws consent for third party access to anonymised personal data

3.6.3 Third Party Reporting Analyst retrieves statistical results for anonymised Volunteer data

3.7 Validation Conclusions

4 Conclusion
List of Figures

Figure 1.1: RestAssured Innovation Pillars ................................................................. 8
Figure 1.2: RestAssured Component Architecture .................................................... 9
Figure 1.3: RestAssured Web and REST Pipeline Reference Example .................. 10
Figure 1.4: RestAssured Stream Pipeline Reference Example ............................. 11

Figure 2.1: PAYD Insurance - current environment (from RestAssured D3.1, Section 3) .... 15
Figure 2.2: PAYD Insurance - potential risks (from RestAssured D3.1, Section 3) ...... 16
Figure 2.3: PAYD Insurance - RestAssured solutions (from RestAssured D3.1, Section 3) ... 17
Figure 2.4: PAYD Insurance - RestAssured solution overview ............................. 18
Figure 2.5: PAYD Insurance use case validation environment overview .................. 21

Figure 3.1: Ami - current environment (from RestAssured D3.1, Section 3) .............. 26
Figure 3.2: Ami - potential risks (from RestAssured D3.1, Section 3) ...................... 27
Figure 3.3: Ami - RestAssured solutions (from RestAssured D3.1, Section 3) .......... 28
Figure 3.4: Ami - RestAssured solution overview ................................................. 28
Figure 3.5: Ami use case validation environment overview ................................. 32
1 Introduction

1.1 Purpose

The purpose of this document is to present the stakeholders and the user stories of the following use cases for the RestAssured project, together with the requirements and validation plans for each of the use cases. As part of the “Use cases and end-user validation” work package (WP8) this document will feed back into the core RestAssured architecture, platform and methodology (WP3) as well as the RestAssured work packages concerning design and implementation of each of the innovation pillars (WP4-7).

- **PAYD**: The Pay As You Drive use case concentrates on securing data streams from connected car sensors, edge devices and untrusted cloud infrastructures used as telematics for usage based automotive insurance with emphasis on compliance to data protection regulations, in particular Regulation (EU) 2016/679 (GDPR).

- **HPC**: The High Performance Computing use case concentrates on securing intellectual property and data integrity across the data lifecycle utilising untrusted infrastructure from cloud service providers where commerical competitors may also be clients. The RestAssured consortium members in conjunction with the RestAssured Project Coordinator have agreed to reschedule the High Performance Computing use case, including its validation planning, to be included in D8.3 Final Validation Plan in the second half of the project.

- **CARE**: The Self-directed Social Care use case concentrates on securing sensitive personal data of vulnerable adults living at home across untrusted, decentralised cloud infrastructures with emphasis on compliance to data protection regulations, in particular Regulation (EU) 2016/679 (GDPR).

![Figure 1.1: RestAssured Innovation Pillars](image-url)
1.2 RestAssured Components

The following summarises the RestAssured architecture component view (from RestAssured deliverable D3.1 - Initial High Level Architecture Release 1.0, Section 6)

![Diagram of RestAssured Component Architecture]

**Figure 1.2: RestAssured Component Architecture**

1.2.1 Orchestration of the RestAssured Components

1. All services register with the RestAssured Service Registry. This must include a description of what they offer (e.g., SGX-enabled service, AMD enclave, PaaS service, etc.), as well as other meta data like physical location, and non-functional properties such as service cost, etc.

2. The application requests a service from the Gatekeeper (e.g., SGX enclave running a secure database instance). The sticky policies (representing constraints on the potential target service) for the data are sent, as well as an identifier confirming the properties of the requester.

3. The Gatekeeper adds any additional sticky policies based on company policy, or legal reasons and queries the Service Registry for the appropriate target.

4. The Service Registry returns the address (i.e., exposes an interface, e.g. REST) to the microservice that meets the requirements.

5. The Gatekeeper creates an access grant containing the authentication information for the requesting service, informing the calling application about the location of the target.

6. The application sends the access grant and requested data to the target service over a secure link, which gets intercepted by the Policy Enforcement Point. If the token is accepted by the Policy Enforcement Point, the information proceeds through, else a reject message is sent.

7. Secure application execution starts (load data, decrypt, process...).

8. The service returns processed results.
1.3 RestAssured Application Microservice Pipeline Reference Examples

RestAssured applications consist of one or more pipelines of microservices registered with the Service Registry of the Trusted Authority (see Figure 1.2). Two reference example application pipelines of multiple mircoservices are outlined, one pipeline for Web and REST API services and a second pipeline for message based data streams.

1.3.1 Web and REST API Pipeline Reference Example

A typical RestAssured application may contain a Web or REST API microservice pipeline (see Figure 1.3) consisting of

- Policy Processor: a data processing microservice that transforms the data as required by the RestAssured sticky policies.
- REST-DB EP Router: a REST to DB Enforcement point and Router that handles encrypted data record storage and decrypted record retrieval with token credentials from the RestAssured Gatekeeper.

The padlocks in Figure 1.3 represent data encryption in transit typically provided by TLS.
1.3.2 Data Stream Pipeline Reference Example

A RestAssured application may require a stream based microservice pipeline following a Map, Filter, Reduce pattern (see Figure 1.4) consisting of

- Map Processor: a Map stream processing microservice.
- Filter Processor: a Filter stream processing microservice.
- Reduce Processor: a Reduce stream processing microservice.
- Stream-DB EP Router: a stream to DB Enforcement Point and Router that handles conversion of processed stream data to encrypted data record storage with token credentials from the RestAssured Gatekeeper.

The padlocks in Figure 1.4 represent data encryption in transit typically provided by TLS.

1.3.3 RestAssured Applications and Multiple Microservice Pipelines

RestAssured applications may consist of multiple routing and processing pipelines, for multiple stakeholder functions, with processing chains of pipelines in serial or parallel.
2 Pay as You Drive: Usage Based Automobile Insurance

2.1 Introduction

An application reaching to the network edge (e.g. Connected Car) that enables the Driver (Data Subject) to identify and limit the transfer of personally identifiable information to the service provider for the purpose of providing usage based car insurance (UBI). This can be attained through the application of policies that match the intent of the data subject to the data, while also enabling the data subject to apply data minimization to certain data (e.g. sensitive data the data subject is not comfortable sharing, or data deemed not to be relevant for the purpose of service contextualization) prior to its transfer to the service provider. Data subjects are able to opt-in/out of secondary/tertiary processing (further processing of the data beyond the original agreed-upon purpose), and the transfer to third party organisations, as per their rights under Regulation (EU) 2016/679 (GDPR).

2.2 State of the Art

2.2.1 Introduction to Usage Based Insurance Models

In the past traditional car insurance policies have used basic static information about driver (age, gender, profession and previous claim history) and automobile (brand, model, year of manufacture) upon which to base premiums for insurance.

“Pay As You Drive (PAYD) describes an automotive usage based insurance product with a pricing model based on distance driven based on telemetric data collected while the car is being driven. The telemetric data set collected for determining the policy premium for such products is often comparatively narrow, mostly limited to odometer readings (distance travelled) and more recently in some cases including geopositioning (GPS) data sets of date, time, speed, direction and location to be used for simplistic usage analysis.

“Pay How You Drive (PHYD) describes a more advanced automotive usage based insurance product with a pricing model based on driver behaviour analysis. The telemetric data set collected for determining the policy premium is a far wider telematic data set (with more resolution and accuracy) and it is processed more deeply than traditional PAYD. Not only using more finely sampled location, time of day, and distance travelled, but also taking in telematics streams of car controls (eg. steering wheel, brakes) instrumentation (tachometer) and other sensors, a driver behavioural profile can be built up algorithmically by back end analysis (such as machine learning) in cloud infrastructures.

Telematic analytics, along with past claims history and locational context, can then factor in determining future policy premiums rates and lead development of future innovative insurance products and services.

This document will use the term PAYD to refer interchangably to all the above insurance models and associated technical components and back-end cloud analysis models.

2.2.1.1 Automotive Dongle

Automotive computerised interfaces have been standard in Europe since Directive 98/69/EC which mandated that from 2004, all newly manufactured petrol and diesel passenger automobiles must be fitted with a standard on board diagnostics interface (called OBD-II) that communicates with built in automobile computerised systems over a Controller Area Network (or CAN bus). Dongle devices used for insurance products include a network communications component, either 3G or 4G to communicate independently or Bluetooth/Wifi to communicate via the drivers smartphone network (usually via a smartphone app). Some of these devices may also contain GPS and accelerometer instuments to provide a richer set of telematic data, to complement the automobiles existing sensor capabilities.
For convenience the interface is often found under the dashboard, once installed, the device usually stays in one vehicle, making dongle based insurance products vehicle centric.

### 2.2.1.2 Smartphone

Modern smartphones contain numerous sensors and instrumentation that are potentially useful in terms of telematics for insurance services, including GPS for location and accelerometers for braking and acceleration.

- **Cuvva** ([https://cuvva.com](https://cuvva.com)) is a traditional PAYD using only a smartphone for telematics, but whose metrics for determining premiums include only residential postcode, age, and hours driven per month. Their unique selling point is that their cover is driver, not vehicle, centric. In particular, their service targets young leaner drivers who borrow cars, families with multiple drivers and car sharers.

### 2.2.1.3 Device Agnostic Telematic UBI

Device Agnostic Telematic Insurance services utilise telematic data streams taken from a variety of devices including automotive dongles and/or smartphones.

- **ByMiles** ([https://www.bymiles.co.uk](https://www.bymiles.co.uk)) is a UK based device agnostic car insurance startup which offers distance driven based automobile insurance, utilising a hardware dongle and/or a Smartphone telematics UBI application.

- **QBE InsuranceBox** ([http://insurancebox.com.au](http://insurancebox.com.au)) is a PHYD based device agnostic UBI insurance service that uses a dongle or smartphone to construct driver behavioural profiles based on parameters including Speed consistency, Acceleration, Braking, and Night driving.

### 2.2.2 Connected Cars

Connected Cars are automobiles that are connected to the Internet (often by 3G or 4G mobile gateways) and provide for interconnectivity to other devices and sensors via technologies such as WiFi and Bluetooth. Connected Cars are beginning to provide onboard virtualisation and container platforms that are capable of providing multi-tenant cloud orchestration and service application deployment into the vehicle itself.

- **Harman** ([http://www.harman.com/](http://www.harman.com/)) is a company that develops Telematics Control Units (TCU) for automobile manufacturers that offer direct interfacing to cloud-based analytics infrastructures via Linux based virtualisation capabilities.

- **Eurotech** ([https://www.eurotech.com](https://www.eurotech.com)) is a company that develops IoT Gateways and Edge servers for Transport and Mobility, bringing standards based cloud orchestration and deployment onto the vehicle.

### 2.2.3 Telematics Service Providers

Telematics Service Providers (TSPs) provide detailed telematic data for automobile insurers, often also offering value added PaaS telematic analytic services for contextual and driver behaviour related risks to the insurers.

It is estimated that the Telematics Service Provider UBI market opportunity will be worth EUR 3 billion globally in 2020[^1].

• The Floow (https://www.thefloow.com) is a device agnostic telematics analysis service provider (PaaS) who collect data from any sensing device, including smartphones stand-alone, in-car devices accessing the OBD-II port and professionally fitted boxes and provide telematics analysis for the automotive insurance industry.

• MyDrive Solutions (http://www.mydrivesolutions.com), is a device agnostic telematics analysis service provider who provide telematics analysis for the automotive insurance industry.
2.3 Gap Analysis

Figure 2.1 illustrates the current (non-RestAssured) dataflow of a telematics based PAYD service with a public cloud service and highlights some of the risks and data protection compliance challenges.

2.3.1 Current Environment

When implemented on untrusted cloud infrastructures, typical PAYD insurance applications (see Figure 2.1) for a connected car pose security and integrity risks, and do not take adequate account of GDPR requirements, especially for the granular protection and access control required upon the dynamic granting or withdrawal of the Driver's informed consent. These include:

- No auditable control measure to protect Insurer Component Driver data processing and database access from untrusted Insurer IaaS and PaaS cloud provider infrastructures (untrusted cloud).
- No auditable control measure to limit Insurer Component Driver data processing and database access from Insurance Analysts based on current state of Driver informed consent (GDPR).

Figure 2.1: PAYD Insurance - current environment (from RestAssured D3.1, Section 3)
- No auditable control measure to protect Telematics Component Driver stream processing and database access from untrusted Telematics IaaS and PaaS cloud provider infrastructures (untrusted cloud).

- No auditable control measure to limit, minimise or block Telematics Component Driver stream processing and historic (or "cold") database access from Telematics Analysts based on current state of Driver informed consent (GDPR).

- No auditable control measure to protect Insurer Component Driver stream processing and database access from untrusted Insurer IaaS and PaaS cloud provider infrastructures (untrusted cloud).

- No auditable control measure to limit, minimise or block Insurer Component Driver stream processing and historic database access from Insurer Analysts based on current state of Driver informed consent (GDPR).

Figure 2.2 illustrates some of the risks of implementing a (non-RestAssured) telematics based PAYD service and the shortfalls and challenges for GDPR compliance in an untrusted cloud environment.

![Figure 2.2: PAYD Insurance - potential risks](image-url)
2.3.2 RestAssured Solution Overview

Figure 2.3 illustrates some of the envisaged security control and risk mitigation measures implementing a RestAssured telematics based PAYD service and the benefits in its support for GDPR compliance in an untrusted cloud environment.

Figure 2.3: PAYD Insurance - RestAssured solutions (from RestAssured D3.1, Section 3)
Figure 2.4: PAYD Insurance - RestAssured solution overview

Figure 2.4 illustrates some of the envisaged security control and risk mitigation components of a RestAssured telematics based PAYD service, itemised below:

- **PAYD Insurer RestAssured REST Pipeline** is an Enforcement Point for sticky policy based database record access control for the PAYD Insurer CryptDB and the RestAssured Gatekeeper only grants access and decryption of the Driver’s encrypted records in accordance with the Driver’s RestAssured sticky policy.

- **Insurer Analytics RestAssured REST Pipeline** is an Enforcement Point for sticky policy based database record access control for the Insurer Analytics Application and the RestAssured Gatekeeper grants access to and decryption of the Driver’s encrypted records in accordance with the Driver’s RestAssured sticky policy.

- **Edge Telematics RestAssured Stream Pipeline** is an Enforcement Point for data stream minimisation in accordance with the Driver’s RestAssured sticky policy generated from the Driver’s privacy settings, providing data stream protection close to the data input source.

- **Telematics RestAssured Stream Pipeline** is an Enforcement Point for data stream minimisation and sticky policy based data stream router sourced from the Driver’s privacy settings and acts as a firewall only allowing policy based minimised data streaming to the Telematics (third party) Analytics database according to the Driver’s privacy settings.

- **Insurer RestAssured Stream Pipeline** is an Enforcement Point for data stream minimisation and sticky policy based data stream router generated from the Driver’s privacy settings and acts as a firewall granting policy based minimised streaming to the Insurer Analytics database according to the Driver’s privacy settings.

- **Telematics Analytics RestAssured REST Pipeline** is an Enforcement Point for sticky policy based database record access control for the Telematics Analytics Application and the RestAssured Gatekeeper grants policy based access to and decryption of the Driver’s encrypted records according to the Driver’s privacy settings.
2.4 Stakeholder Definitions and Stories

For a telematic insurance service, there exist many possible combinations of stakeholder representations, responsibilities and relationships. What follows is one possible configuration.

The chosen validation environment consists of stakeholders where:

- A Driver desires an insurance product and wishes to directly engage with and provide information to an Insurance Service Provider.

- The Insurance Service Provider engages a Telematics Service provider to manage delivery of Driver data streams to the Insurance Service Provider’s infrastructure. The Telematics Service provider has no prior or existing relationship to the Driver.

- Both the Insurance Service Provider and the Telematics Service Provider individually engage Cloud Infrastructure providers (IaaS and PaaS) as part of their infrastructure that supports the insurance service provided by the Insurance Service Provider to the Driver.

2.4.1 Driver

The Driver(s) are the one or more drivers authorised to be covered within a given automobile insurance policy product offered by the Insurance Service Provider. Within the context of the GDPR, the drivers of the automobile are Data Subjects and control data exposure and flow through their privacy settings.

1. As a driver I want a cost effective, usage based automotive insurance service.

2. As a driver I want to manage my personal data through the privacy settings for the usage based insurance service.

3. As a driver I want to understand and manage who will access and for what reasons my personal data is processed to ensure that my insurance product privacy settings match my informed consent.

4. As a driver I want my granting or withdrawal of informed consent for the insurance service to take effect in a timely manner.

5. As a driver I want to be notified when the service provider change policies for data storage, exchange and processing so I can keep my informed consent up to date and select product privacy settings accordingly.

2.4.2 Insurance Service Provider

The Insurance Service Provider (Insurer) is the provider of the automobile insurance product to the Driver. Within the context of the GDPR, the Service Provider is a Data Controller.

1. As an insurance service provider I want to offer innovative, cost effective, dynamic usage based automotive insurance services.

2. As an insurance service provider I want customer data streams processed sufficiently to offer dynamic and competitive premiums for telematic usage based insurance service offerings.

3. As an insurance service provider I want to comply with EU wide personal data and privacy frameworks (GDPR) in offering clear and accurate personal data usage description within the insurance service to facilitate informed consent of the products privacy settings.
4. As an service provider I want to maintain non-repudiable personal data storage, exchange and processing event audit trails to sufficiently demonstrate secure compliance to personal data and privacy regulations (GDPR).

5. As an insurance service provider I want to maintain non-repudiable audit trail of all changes to customer privacy settings.

6. As an insurance service provider I want to act upon Driver granting or withdrawal of informed consent in a timely manner.

7. As an insurance service provider I want to notify customers in a timely manner of any policy or product change that may affect their personal data privacy settings and prompt for renewal of informed consent.

2.4.3 Telematics Provider

The Telematics Provider is the provider of streamed telematic data from the Driver’s connected car to the Insurance Service Provider. With authorisation of the Insurance Service Provider and freely informed consent of each participating Driver, the telematics provider may desire access to Driver connected car data for defined analytic purposes. Within the context of the GDPR, the Telematics Provider is a Data Processor (data routing to Insurer) and Data Controller (for data stored by consenting Drivers).

1. As a telematics provider I want to provide cost effective automotive data stream delivery services for the Service Provider.

2. As a telematics provider, with Driver informed consent, I want to use driver data for a clearly defined use.

3. As a telematics provider and data processor, I want to maintain non-repudiable personal data storage, exchange and processing event audit trails to sufficiently demonstrate secure compliance to personal data and privacy regulations (GDPR).

2.4.4 Insurer and Telematics Infrastructure as a Service (IaaS) Providers

The Infrastructure as a Service Providers provide untrusted cloud infrastructures to the service providers, and the RestAssured solution allows them to offer a more secure service compliant with data protection regulations such as the GDPR.

1. As an IaaS provider I want to offer cloud infrastructure services that provide security features to allow Service Providers as customers to comply with EU data protection and privacy regulations (GDPR).

2. I want to offer secure cloud infrastructure services that cannot expose sensitive data or data processing to the cloud infrastructure itself outside the Service Provider’s secured domain of control.

2.4.5 Insurer and Telematics Platform as a Service (PaaS) Providers

The Platform as a Service Providers provide untrusted cloud platforms to the service providers, and the RestAssured solution allows them to offer a more secure service compliant with data protection regulations such as the GDPR.

1. As an PaaS provider I want to provide Cloud Platform services that provide auditable cloud security features to allow Service Providers as customers to comply with EU data protection and privacy regulations.
2. I want to offer secure cloud platform services that cannot expose sensitive data or data processing to the cloud platform or infrastructure itself outside the Service Provider’s secured domain of control.

2.5 Validation Environment Overview

The PAYD use case validation environment will be connected to a validation instance of the RestAssured core system (Trusted Authority consisting of a Gatekeeper and Service Registry - see Section 1.2) preconfigured with all necessary configurations for the validation testing to occur.

![Figure 2.5: PAYD Insurance use case validation environment overview](image)

The PAYD use case validation environment contains two major differences to a deployed solution (see Figure 2.4).

1. For ethical considerations concerning the handling of PII, synthetic insurance profiles will be created and synthetic and simulator-based automobile telematics will be used in the validation environment. See “PAYD Synthetic Driver Input” and “Automobile Simulator and Synthetic Input / Stream Output” in Figure 2.5.

2. In order to audit Driver personal settings against RestAssured sticky policy data access and flow changes, validation probes may require specific single data encryption paths or other control mechanisms to be disabled or modified to allow the clear-text validation of correct use case scenario results to occur (see probe points highlighted in Figure 2.5).

2.6 Validation Scenarios

The following set of validation scenarios are based on one particular set of business relationships (see Section 2.4), but cover key technical requirements that affect many potential PAYD business value networks.
2.6.1 Driver grants consent for Telematics Provider access to telematic data

With informed consent, the Driver changes their privacy settings for the service to allow the Telematics Service Provider (third party) use of their telematic data for explicitly defined and clearly explained further use.

2.6.1.1 Expected Actions

The Driver’s new privacy settings for the insurance service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate legal and application policies with the new Driver policy creating a new sticky policy (see Section 1.2). The RestAssured Gatekeeper provides authorisation for the Telematics Provider’s RestAssured Streaming Pipeline to route the streaming data to the Telematic Providers encrypted database. The RestAssured Gateway allows the Telematics Analysis Pipeline access to the Driver’s stored encrypted database records.

2.6.1.2 Validation Checklist

1. The Driver’s telematics data stream content received by the Telematics encrypted database must be audited against the Driver’s new privacy settings reflected in the new sticky policy to allow access (see Section 2.4.2 item [3]). The Telematics Stream Probe is used to verify that only the Driver data authorised by the Driver privacy settings is added to the Telematics CryptDB.

2. The Telematics Analyst Pipeline access to the Driver’s records in the Telematics CryptDB must be audited against the Driver’s new privacy settings reflected in the new sticky policy (see Section 2.4.1 item [2]). The Telematics DB Access probe is used to verify that only the data authorised by the Driver privacy settings is available to the Telematics Analytics Application.

3. The Driver’s new privacy settings must allow stream routing and grant encrypted database access of Driver records to the Telematics Provider in a timely manner (see Section 2.4.1 item [4]). The timeliness is measured as the time difference between the Driver privacy setting change and the change in the Driver telematics stream detected by the Telematics Stream probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

4. The RestAssured non-repudiable audit log must be updated to reflect the driver’s new privacy settings (see Section 2.4.2 item [5]).

2.6.2 Driver withdraws consent for Telematics Provider access to telematic data

The Driver changes their privacy settings for the service to block the Telematics Service Provider (third party) use of their telematic data.

2.6.2.1 Expected Actions

The Driver’s new privacy settings for the insurance service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate legal and application policies with the new driver policy creating a new sticky policy (see Section 1.2). The RestAssured Gatekeeper denies authorisation for the Telematics Provider’s RestAssured Streaming Pipeline to route the streaming data to the Telematic Providers encrypted database. The RestAssured Gateway denies the Telematics Analysis Pipeline access to the Driver’s stored encrypted database records.
2.6.2.2 Validation Checklist

1. The Driver’s telematics data stream content received by the Telematics encrypted database must be audited against the Driver’s new privacy settings reflected in the new sticky policy to block access (see Section 2.4.2 item 3).

2. The Telematics Analyst Pipeline access to the Driver’s records in the Telematics CryptDB must be audited against the Driver’s new privacy settings reflected in the new sticky policy.

3. The Driver’s new privacy settings must allow stream routing and grant encrypted database access of Driver records to the Telematics Provider in a timely manner (see Section 2.4.1 item 4). The timeliness is measured as the time difference between the Driver privacy setting change and the change in the Driver telematics stream detected by the Telematics Stream probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

4. The RestAssured non-repudiable audit log must be updated to reflect the driver’s new privacy settings (see Section 2.4.2 item 5).

2.6.3 Driver grants consent for Telematics Provider for aggregate use

With informed consent, the Driver changes their privacy settings for the service to allow the Telematics Service Provider (third party) use of their telematic data stream for explicitly defined and clearly explained aggregate use.

2.6.3.1 Expected Actions

The Driver’s new privacy settings for the insurance service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate legal and application policies with the new Driver policy creating a new sticky policy (see Section 1.2). The RestAssured Gatekeeper provides authorisation for the Telematics Provider’s RestAssured Streaming Pipeline to route data to be aggregated the Telematic Providers encrypted database. The RestAssured Gateway allows the Telematics Analysis Pipeline access to the Driver’s stored encrypted database for aggregate use.

2.6.3.2 Validation Checklist

1. The Driver’s telematics data stream content received by the Telematics encrypted database must be audited against the Driver’s new privacy settings reflected in the new sticky policy to allow aggregate access only (see Section 2.4.2 item 3). The Telematics Stream Probe is used to verify that only the Driver data authorised by the Driver privacy settings is added to the Telematics CryptDB.

2. The Telematics Analyst Pipeline access to the Driver’s records in the Telematics CryptDB must be audited against the Driver’s new privacy settings reflected in the new sticky policy (see Section 2.4.1 item 4). The Telematics DB Access probe is used to verify that only the aggregate data access authorised by the Driver privacy settings is available to the Telematics Analytics Application.

3. The Driver’s new privacy settings must allow stream routing and grant database access of aggregate Driver records to the Telematics Provider in a timely manner (see Section 2.4.1 item 4). The timeliness is measured as the time difference between the Driver privacy setting change and the change in the Driver telematics stream detected by the Telematics Stream probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

4. The RestAssured non-repudiable audit log must be updated to reflect the driver’s new privacy settings (see Section 2.4.2 item 5).
2.6.4 Driver grants consent for Telematics Provider for anonymous use

With informed consent, the Driver changes their privacy settings for the service to allow the Telematics Service Provider (third party) use of their telematic data stream for explicitly defined and clearly explained anonymous use.

2.6.4.1 Expected Actions

The Driver’s new privacy settings for the insurance service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate legal and application policies with the new Driver policy creating a new sticky policy (see Section 2.2). The RestAssured Gatekeeper provides authorisation for the Telematics Provider’s RestAssured Streaming Pipeline to anonymise and route data to the Telematic Providers encrypted database. The RestAssured Gateway allows the Telematics Analysis Pipeline access to the Driver’s stored database anonymised data records.

2.6.4.2 Validation Checklist

1. The Driver’s telematics anonymous data stream content received by the Telematics encrypted database must be audited against the Driver’s new privacy settings reflected in the new sticky policy to allow anonymised data only (see Section 2.4.2 item 3). The Telematics Stream Probe is used to verify that only the Driver data authorised by the Driver privacy settings is added to the Telematics CryptDB.

2. The Telematics Analyst Pipeline access to the Driver’s records in the Telematics CryptDB must be audited against the Driver’s new privacy settings reflected in the new sticky policy (see Section 2.4.1 item 2). The Telematics DB Access probe is used to verify that anonymised data authorised by the Driver privacy settings is available to the Telematics Analytics Application.

3. The Driver’s new privacy settings must allow stream routing and grant encrypted database access of Driver records to the Telematics Provider in a timely manner (see Section 2.4.1 item 4). The timeliness is measured as the time difference between the Driver privacy setting change and the change in the Driver telematics stream detected by the Telematics Stream probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

4. The RestAssured non-repudiable audit log must be updated to reflect the driver’s new privacy settings (see Section 2.4.2 item 5).

2.7 Validation Conclusions

The successful validation of the selected scenarios of RestAssued PAYD Insurance use case demonstrates that

- the RestAssured architecture will assist in the secure leveraging of public untrusted cloud infrastructures whilst maintaining security and data protection regulatory requirements across multiple stakeholder value chains.

- variations of the PAYD use case would be applicable to many other business value networks and data lifecycle models, of which the above validation scenarios form a representative case study.

- the RestAssured solution can be applied to other systems requiring secure data streams, notably IoT data streams that can exploited in IoT vertical markets where data streams passing though multiple stakeholders can be secured in public cloud infrastructures whilst maintaining compliance to data protection regulations.
3 CARE: Self Directed Social Care

3.1 Introduction

A web-based application that matches service providing volunteers with people requiring help (clients). Both the volunteers and the clients (on their behalf by third party volunteer organisations) provide personal data (i.e. are data subjects). The application matches the volunteer with clients based on their search criteria (location, interests etc.). When a volunteer finds someone that they’d like to help, the application will advise them which volunteer organisation that client is registered with and invite them to sign up with the same organisation, who will contact the volunteer to arrange an interview, DBS checks, references etc.

Third parties are also allowed to register with Ami to run reports relating to anonymised volunteer data, for example a Local Authority may wish to identify client needs in specific areas. Only the data that volunteers have permitted to be shared should be accessible to the third party.

3.2 State of the Art

3.2.1 Introduction to Self-Directed Social Care (Ami)

The procurement and monitoring of social care is a complex interaction of several stakeholders sharing a citizens sensitive personal data: the service user, their family and carers, social care providers (for-profit companies and not-for-profit charities), and the Local Authority. (In the UK, a Local Authority or LA is the government organisation officially responsible for public services and facilities in a particular locality.)

Information is usually stored by the organizations involved (usually the LA and service providers) on premise and is rarely placed in the cloud. Blanket privacy statements to which the citizen is assumed to have consented control the data. In general, local authorities and service providers are required to adhere to data protection laws with little specialist knowledge. The cultural distrust of cloud storage by stakeholders is an obstacle to the efficient sharing and use of personal data necessary to make self-directed support a reality.

The RestAssured UK use case concerns the setting up of care to vulnerable adults living at home which requires personal data to be shared securely and easily between stakeholders. There is also a need for anonymised data to be provided to service commissioners within the WLA to monitor the services.

3.3 Gap Analysis

Figure [3.1] illustrates the current (non-RestAssured) data flow of a social-care volunteering service with a public cloud service and highlights some of the risks and data protection compliance challenges.
3.3.1 Current Environment

There are a number of potential data security and integrity risks for the current implementation of self-directed social care, when using an untrusted cloud infrastructure. Furthermore the current solution does not take adequate account of GDPR requirements, especially for the granular protection and access control required upon the dynamic granting or withdrawal of the Volunteer’s informed consent for data sharing. These include:

- No auditable control measure to protect Ami Component Volunteer data processing and database access from untrusted Ami IaaS and PaaS cloud provider infrastructure (untrusted cloud).
- No auditable control measure to limit Ami Component Volunteer data processing and database access from Third Party Reporting Analysts based on current state of Volunteer informed consent (GDPR).
- No auditable control measure to limit Ami Component Volunteer data processing and database access from Volunteer Organisations based on current state of Volunteer informed consent (GDPR).

Figure 3.1: Ami - current environment (from RestAssured D3.1, Section 3)
Figure 3.2: Ami - potential risks (from RestAssured D3.1, Section 3)

Some of the data security and integrity risks associated with the current (non-RestAssured) implementation, in an untrusted cloud, including some of the GDPR compliance challenges are highlighted in Figure 3.2.

3.3.2 RestAssured Solution Overview

Figure 3.3 illustrates some of the security control and risk mitigation measures for a RestAssured self-directed social care implementation and the benefits in its support for GDPR compliance in an untrusted cloud environment.
Figure 3.3: Ami - RestAssured solutions (from RestAssured D3.1, Section 3)

Figure 3.4: Ami - RestAssured solution overview
The security control and risk mitigation components of a RestAssured self-directed social care service implementation are illustrated in Figure 3.4 and are itemised below:

- Ami RestAssured REST Pipeline is an Enforcement Point for sticky policy based database record access control for the Ami Encrypted Database. The RestAssured Gatekeeper only grants access and decryption of the Volunteer’s encrypted records in accordance with the Volunteer’s RestAssured sticky policy.

- Ami Reporting RestAssured REST Pipeline is an Enforcement Point for sticky policy based database record access control for the Ami Reporting Service. The RestAssured Gatekeeper grants access to and decryption of the Volunteer’s encrypted records in accordance with the Volunteer’s RestAssured sticky policy.

- Third Party Reporting RestAssured REST Pipeline is an Enforcement Point for sticky policy based database record access control for the Third Party Reporting Application. The RestAssured Gatekeeper grants policy based access to and decryption of the Volunteer’s encrypted records according to the Volunteer’s privacy settings.

### 3.4 Stakeholder Definitions and Stories

#### 3.4.1 Volunteer

The volunteer, or service user, provides personal data to the Service Provider when registering with Ami. Within the context of the GDPR, the volunteer is both a Data Subject and Data Consumer.

1. As a volunteer I want to find clients that match my criteria so that I can offer them assistance.
2. As a volunteer I want to view and change my privacy settings so that I can control who has access to my data.
3. As a volunteer I want to trust the organisation that stores my data so that I feel that it is secure.
4. As a volunteer I want to view who has accessed my data and for what reasons so that I can ensure that it matches my preferences.
5. As a volunteer I want to understand the terms by which my data is stored so that I can understand which preferences I should set.
6. As a volunteer I want to be notified when the policies for data storage/usage change so that I can amend my preferences accordingly.
7. As a volunteer I want to be notified when an organisation wishes to access my data so that I can refine my preferences.
8. As a volunteer I want my changes to my privacy preferences to take effect in a timely manner.
9. As a volunteer I want to use as little time as possible to secure my data so that I complete the process quickly.
3.4.2 Client

The client provides personal data to the Service Provider via a third party volunteer organisation. Within the context of the GDPR, the client is both a Data Subject and Data Consumer.

1. As a client I want to be matched with volunteers so that I receive relevant assistance.

2. As a client I want someone else to be able to sign up for me so that I don’t have to use a computer or travel.

3. As a client I want someone else to be able to manage my preferences and data so that I don’t have to use a computer.

4. As a client I want to trust the organisation that stores my data so that I feel that it is secure.

3.4.3 Third Party Volunteer Organisation

The third party volunteer organisation provides personal data to the Service Provider on behalf of the client. The volunteer organisation receives volunteer and client data from the Service Provider in the form of anonymised reports. Within the context of the GDPR, the volunteer organisation is both a Data Consumer and Data Controller.

1. As a volunteer organisation I want to match volunteers and clients automatically so that assistance can be given to more clients.

2. As a volunteer organisation I want to be able to run reports on volunteer data so that I can monitor client social care needs and the types of volunteers in a geographical area.

3. As a volunteer organisation I want to make the process of signing up a volunteer/client quick so that I can use the minimum resource.

4. As a volunteer organisation I want to trust that the Service Provider manages client and volunteer data as per legislation.

3.4.4 Local Authority

The Local Authority receives and processes volunteer and client data from the Service Provider in the form of anonymised reports. Within the context of the GDPR, the Local Authority is both a Data Consumer and Data Controller.

1. As a Local Authority I want to be able to run reports on volunteer and client data so that I can monitor client social care needs and the types of volunteers in a geographical area.

2. As a Local Authority I want to ensure that there are no data breaches so that I do not lose reputation.

3.4.5 Service Provider

The Service Provider is the provider of the volunteer and client matching service and is provided with information from the Data Subjects, and gives information to the Data Consumer. Within the context of the GDPR, the Service Provider is a Data Controller.

1. As a service provider I want to offer a secure and cost effective method for volunteers to be matched with clients automatically.
2. As a service provider I want to comply with EU wide personal data and privacy frameworks (GDPR) in offering clear and accurate personal data usage description within the Ami service to facilitate informed consent of the product’s privacy settings.

3. As a service provider I want to maintain non-repudiable personal data storage, exchange and processing event audit trails to sufficiently demonstrate secure compliance to personal data and privacy regulations (GDPR).

4. As a service provider and data controller I want all data processors to also maintain non-repudiable personal data storage, exchange and processing event audit trails that sufficiently demonstrate secure compliance to personal data and privacy regulations (GDPR).

5. As a service provider and data controller I want to ensure that anonymised data cannot be de-anonymised when passed to third parties.

6. As a service provider I want to ensure that there are no data breaches so that I do not lose reputation.

7. As a service provider I want to maintain a non-repudiable audit trail of all changes to volunteer privacy preferences.

8. As a service provider I want to notify volunteers in a timely manner of any policy or product change that may affect their personal data privacy preferences and prompt for renewal of informed consent.

9. As a service provider I want to act upon volunteer privacy preference changes in a timely manner.

3.4.6 Infrastructure as a Service (IaaS) Provider

The Infrastructure as a Service Providers provide untrusted cloud infrastructures to the service providers, and the RestAssured solution allows them to offer a more secure service compliant with data protection regulations such as the GDPR.

1. As an IaaS provider I want to offer cloud infrastructure services that provide security features to allow Service Providers as customers to comply with EU data protection and privacy regulations (GDPR).

2. I want to offer secure cloud infrastructure services that cannot expose sensitive data or data processing to the infrastructure itself outside the Service Provider’s secured domain of control.

3.4.7 Platform as a Service (PaaS) Provider

The Platform as a Service Providers provide untrusted cloud platforms to the service providers, and the RestAssured solution allows them to offer a more secure service compliant with data protection regulations such as the GDPR.

1. As an PaaS provider I want to provide Cloud Platform services that provide auditable cloud security features to allow Service Providers as customers to comply with EU data protection and privacy regulations.

3.5 Validation Environment Overview

The Ami self-directed social care use case validation environment will be connected to a validation instance of the RestAssured core system (Trusted Authority consisting of a Gatekeeper and Service Registry - see Figure 1.2) preconfigured with all necessary configurations for the validation testing to occur.
The Ami use case validation environment is detailed in Figure 3.5.

**Figure 3.5: Ami use case validation environment overview**

The Ami use case validation environment differs to the solution presented in Figure 3.4 as follows:

1. The Ami validation use case will initially focus on the Third Party Reporting services. By focusing on the reporting services, the existing Ami application can be more easily adapted within budgetary constraints to utilise all RestAssured security control and risk mitigation measures. Furthermore, this will allow the RestAssured technologies be tested fully.

2. For ethical considerations concerning the handling of PII (Personally Identifiable Information), synthetic volunteer and client data will be created and used in the validation environment.

3. In order to audit Volunteer personal settings against RestAssured sticky policy data access and flow changes, validation probes may require specific single data encryption paths or other control mechanisms to be disabled or modified to allow the clear-text validation of correct use case scenario results to occur (see probe points highlighted in Figure 3.5).

The diagram expands on the Third Party Reporting environment presented in Figure 3.4. In this environment the central Ami system (including volunteer web application and database) is considered to be implemented on a secure and trusted platform. The reporting services are hosted in an untrusted cloud environment and have been named the “Social Care Analysis of Needs Tool” (SCANT).

This tool allows authorised third parties (Local Authorities and Volunteer Organisations) to retrieve statistical results of volunteer data in anonymised form. Only data which a Volunteer has given their informed consent for sharing can be accessed by the third party. The data is encrypted and access is secured and audited through the RestAssured components.
3.6 Validation Scenarios

3.6.1 Volunteer grants consent for third party access to anonymised personal data

With informed consent, the volunteer changes their personal data privacy settings for Ami to allow a third party (e.g. the Local Authority or Volunteer Organisation) to use their anonymised personal data for explicitly defined and clearly explained anonymous use.

3.6.1.1 Expected Actions

The Volunteer’s new privacy settings for the Ami service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate Legal and Application policies with the new Volunteer policy creating a new sticky policy (see Section 1.2). The RestAssured Gateway allows the third party access to the volunteer’s anonymised data.

3.6.1.2 Validation Checklist

1. The RestAssured non-repudiable audit log must be updated to reflect the Volunteer’s new privacy settings (see Section 3.4.5 item 7).

2. The third party’s access to volunteer data must be audited against the Volunteer’s new privacy settings reflected in the new sticky policy to allow access (see Section 3.4.1 item 2). The SCANT Database Access probe (see Figure 3.5) is used to verify that only the data authorised by the Volunteer privacy settings is available to the SCANT Application.

3. The Volunteer’s new privacy settings must allow access of volunteer data to the third party report analyst in a timely manner (see Section 3.4.1 item 8). The timeliness is measured as the time difference between the Volunteer privacy setting change and the change in the Reporting Service detected by the SCANT Database Access probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

3.6.2 Volunteer withdraws consent for third party access to anonymised personal data

The volunteer changes their privacy settings to block third party (e.g. the Local Authority or Volunteer Organisation) use of their anonymised personal data.

3.6.2.1 Expected Actions

The Volunteer’s new privacy settings for the Ami service are submitted to the RestAssured Gatekeeper, which blends the existing appropriate Legal and Application policies with the new Volunteer policy creating a new sticky policy. The RestAssured Gateway blocks the third party access to the volunteer’s anonymised data.

3.6.2.2 Validation Checklist

1. The RestAssured non-repudiable audit log must be updated to reflect the Volunteer’s new privacy settings (see Section 3.4.5 item 7).

2. The third party’s access to volunteer data must be audited against the Volunteer’s new privacy settings reflected in the new sticky policy to block access (see Section 3.4.1 item 2). The SCANT Database Access probe is used to verify that only the data authorised by the Volunteer privacy settings is available to the SCANT Application.
3. The Volunteer’s new privacy settings must block access of volunteer data to the third party report viewer in a timely manner (see Section 3.4.1 item 8). The timeliness is measured as the time difference between the Volunteer privacy setting change and the change in the Reporting Service detected by the SCANT Database Access probe. The timeliness results will be assessed in D8.2 - Initial Validation Results before the final validation phases begin.

3.6.3 Third Party Reporting Analyst retrieves statistical results for anonymised Volunteer data

The Third Party Reporting Analyst (an employee of a Local Authority or authorised Volunteer Organisation) carries out a report for statistical results of specific Volunteer data types for further analysis.

3.6.3.1 Expected Actions

A third party should not be provided with statistical results of anonymised Volunteer personal data if the amount of data subjects, whose data is included in the results allows de-anonymisation, and thus re-identification of the associated data subjects. The anonymised data that the third party is granted access to is said to have the k-anonymity property if the personal information about each data subject included in the data cannot be differentiated from at least k-1 data subjects that also have their data included in the anonymised data.

3.6.3.2 Validation Checklist

1. The third party’s access to volunteer data must be audited against k-anonymisation measures to detect when the k-anonymity property is missing (see Section 3.4.5 item 5). The SCANT k-anonymity probe (see Figure 3.5) is used to verify that anonymised data that does not meet the k-anonymisation requirement is identified.

2. The third party’s access to volunteer data must be blocked when the anonymised data is identified as not possessing the k-anonymity property. The SCANT Database Access probe is used to verify that only the data that meets the k-anonymity measure is available to the SCANT Application.

3.7 Validation Conclusions

The successful validation of the selected scenarios of RestAssued Self-Directed Social Care use case demonstrates that

- the RestAssured architecture assists in secure leveraging of public untrusted cloud infrastructures whilst maintaining security and data protection regulatory requirements across multiple stakeholder value chains.

- the RestAssured solution can be applied to other systems requiring sensitive personal data reporting with anonymisation, can be secured in public cloud infrastructures whilst maintaining compliance to data protection regulations.
4 Conclusion

The initial end user validation results will contribute to the evaluation of the RestAssured software stack across a wide range of complex real world use cases and will assist in the secure leveraging of public untrusted cloud infrastructures whilst maintaining security and data protection regulatory requirements.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Data Protection Concern</th>
<th>Cloud Architecture</th>
<th>Involved Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>CARE: Self-directed Social Care</td>
<td>Privacy and de-anonymization (sensitive personally identifiable data)</td>
<td>Public, decentralized cloud</td>
<td>Vulnerable adults living at home; social care providers</td>
</tr>
<tr>
<td>PAYD: Pay As You Drive</td>
<td>Privacy (personally identifiable data)</td>
<td>Sensors, edge devices, and cloud</td>
<td>Drivers; Telematics and insurance providers</td>
</tr>
<tr>
<td>HPC: High Performance Computing for Commercial Use</td>
<td>IPR (business sensitive data)</td>
<td>Data centre (possibly federated)</td>
<td>Commercial enterprises; High performance computing centres</td>
</tr>
</tbody>
</table>

The breadth of the use cases and their validation will indicate applicability of the RestAssured framework to many other business value networks and data lifecycle models, and form a set of representative case studies where data passing though multiple stakeholders can be secured in public cloud infrastructures whilst maintaining security standards for treatment of commercially sensitive data as well as compliance to data protection regulations such as Regulation (EU) 2016/679 (GDPR).