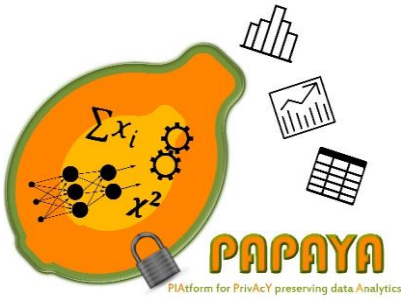

D1.4 – SECOND PROJECT PROGRESS REPORT

Work Package	WP 1, Project Management
Lead Author	Melek ÖNEN (EURC)
Contributing Author(s)	Eleonora Ciceri (MCI), Marco Mosconi (MCI), Boris Rozenberg (IBM), Ángel Palomares (ATOS), Dmitry Pap (ATOS), Sébastien Canard (ORA), Simone Fisher-Hübner (KAU), Tobias Pulls (KAU)
Reviewers	All
Due date	30.04.2020
Date	01.12.2021
Version	2.0
Dissemination Level	Public version

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767. The content and results of this deliverable reflect the view of the consortium only. The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Project No. 786767

Revision History

Revision	Date	Editor	Notes
0.1	17.03.2020	Melek Önen (EURC)	First version with todos
0.2	06.04.2020	Melek Önen (EURC), Boris Rozenberg (IBM), Dmitry Pap (ATOS), Eleonora Ciceri (MCI)	Second version with todos.
0.3	14.04.2020	Melek Önen (EURC), Boris Rozenberg (IBM), Eleonora Ciceri (MCI), Ángel Palomares (ATOS), Dmitriy Pap (ATOS), Sébastien Canard (ORA)	Third version with todos
0.4	22.04.2020	Melek Önen (EURC), Boris Rozenberg (IBM), Ángel Palomares (ATOS), Sébastien Canard (ORA), Eleonora Ciceri, Simone Fischer-Hübner (KAU)	V4 with todos
1.0	30.04.2020	Melek Önen (EURC), Boris Rozenberg (IBM), Ángel Palomares (ATOS), Sébastien Canard (ORA), Eleonora Ciceri, Simone Fischer-Hübner (KAU)	Final version

Table of Contents

List of Tables

List of Figures

Executive Summary

This deliverable overviews the project's second year activities, namely from May 1st, 2019 to April 30th, 2020. As a reminder, the main goal of PAPAYA is to design and develop a **platform of privacy preserving analytics modules** that allows the outsourcing of analytics operations into untrusted cloud servers while protecting the privacy of the data. Thanks to these newly developed platform, stakeholders will be able to ensure their clients' privacy (and be compliant with the General Data Protection Regulation) while extracting valuable and meaningful information from the analyzed data.

The second year project activities reported in this document can be summarized as follows:

- On the technical side, **WP3** that aims at developing the privacy enhancing technologies for data analytics has successfully ended. The project has developed privacy preserving variants of a group of **four** analytics namely **neural networks** (classification, collaborative training), **trajectory clustering, counting** and **basic statistics**. These modules use different cryptographic tools such as homomorphic encryption, differential privacy or functional encryption and target different settings (single data owner, multiple data owners, e.g.). The specification of these primitives is reported in deliverable **D3.3,** submitted in M24. Additionally, various **user interfaces (UI**) have also been developed to enhance transparency with regards to data subjects and other stakeholders. These are presented in deliverable **D3.4** (submitted in M24) and include: (i) an extension of the CNIL's Privacy Impact Assessment (PIA) tool that helps PAPAYA stakeholders assess the impact of privacy preserving analytics on privacy and security goals. The tool is also rendered more clear to data subjects; (ii) UIs that explain how PAPAYA privacy preserving analytics work; (iii) a privacy engine tool takes data subject's privacy preferences and rights into account. Consequently, **MS3: PAPAYA analytics implementation** and **MS4: PAPAYA transparency method description** are achieved. Furthermore, **WP4** aims at developing the integrated platform. The architecture of the overall PAPAYA platform including the dashboard is specified and reported in deliverable **D4.1.** The progress on the integration of PETs specified in WP3 are reported in deliverable **D4.2** submitted in M24.
- Regarding activities related to **innovation management**, since the development of various PAPAYA components has become more mature, identified innovation assets and responses to innovation questionnaires have been updated. These are reported in section 3. Potential patents and contribution to standards are also identified. Finally, **D6.4** describes the value proposition of the project outcomes (with respect to **D1.2** and the marketing questionnaires) and the market analysis (segmentation, PEST analysis, competitors and SWOT). **D6.4** does not include updated the second version of innovation questionnaires as it was released beforehand.
- Finally, the second year's **dissemination and communication activities** consist of the organization of and participation to various events including scientific conferences, workshops, forums and summer schools. There are now eight scientific publications.

PAPAYA actively collaborates with other EU projects and is a now a member of the GDPR cluster.

Glossary of Terms

ATOS	Atos Spain S.A.
CNIL	Commission Nationale de l'Informatique et des Libertés
DoA	Description of Actions
EURC	EURECOM
GDPR	General Data Protection Regulation
IBM	IBM Israel Science & Technology Ltd.
KAU	Karlstad University
M	Month
MCI	Mediaclinics Italia
MS	Milestone
O	Objective
ORA	Orange
PAPAYA	PlAtform for PrivAcY preserving data Analytics
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
SotA	State-of-the Art
UC	Use Case
UI	User Interface
WP	Work Package
Y2	Year 2

1 Introduction

1.1 Purpose and Scope

As a reminder, the goal of the PAPAYA project is to devise and develop a **platform of privacy preserving modules** that protects the **privacy of users** on an end-to-end basis without sacrificing **data analytics functionalities**. The PAPAYA framework will integrate several privacy preserving data analytics modules each of them dedicated to specific analytics operations and to specific settings (single data owner, multiple data owners, etc.). The platform aims to be usable in the sense that it also includes proper transparency and control mechanisms through a dashboard.

During the second year of the project, the major activities consist of the design and development of the privacy enhancing technologies for data analytics including the transparency and control mechanisms (WP3) and the specification of the overall architecture of the actual PAPAYA platform (WP4), the beginning of its implementation and the integration of some of the WP3 modules. Furthermore, dissemination and communication activities have also been continuing to promote the project's objectives, innovation aspects and results. The exploitation strategy of each different identified assets has also been defined and some initial activities have already started (WP6).

1.2 Outline

Similar to deliverable D1.3, the document first summarizes the progress in terms of technical contributions (Section 2) and innovation management (Section 3). The second year's dissemination, communication and exploitation activities are then reported in Section 4. The work carried on by all partners is further described in details in section 5, in a Work Package and Task basis. Section 6 reviews the recommendations and comments provided by the EC and the reviewers during the first review of the project and provides some responses to each of them. Finally, section 7 reviews the status of all project deliverables, milestones and risks relevant to the second year.

2 Overall Scientific Progress

2.1 Objectives

As a reminder, the project considers the following objectives:

- **O1:** Design efficient **privacy-preserving data analytics** techniques
- **O2:** Explore **different settings** (single/multiple data sources, …)
- **O3:** Enable **risk management** and **user control** of data disclosure
- **O4:** Design and develop an **integrated platform**
- **O5:** Lead an **end-to-end analysis** for different use cases regrouped in two umbrellas: analytics for **healthcare** and **mobile and phone usage** analytics
- **O6: Disseminate** and **exploit** the project outcomes.

In the sequel of this section, we describe the work carried out during the second year of the project towards the achievement of each scientific objective.

2.2 Design of efficient privacy preserving data analytics techniques (O1)

As part of WP3, the design and development of each individual privacy preserving analytics module (privacy preserving Neural Network (NN) classification, privacy preserving collaborative training, privacy preserving trajectory clustering, privacy preserving counting) is completed and reported in deliverable D3.3. These modules have also been evaluated in terms of privacy, performance and accuracy. In particular, a comparative performance study has been conducted for the four privacy preserving NN classification modules.

2.3 Exploration of different restricted settings and design of dedicated protocols (O2)

As mentioned in the previous progress report, each PAPAYA use case described in D2.2 targets different settings. Each use case will also make use of different privacy preserving data analytics. The annex document of D4.1 illustrates the various modules that will be used at each use case.

2.4 Risk management and user-control of data disclosure (O3)

D3.2 reports on the technical design of transparency and risk components and the Privacy Engine. Firstly, a number of risk artefacts are identified based on privacy risk analyses that may be suitable for conveying risks to users. Moreover, the literature has been reviewed on the explanation of trade-offs between privacy and utility in privacy-preserving analytics and on the explanation of the privacy preserving data analytics modules. Finally, the technical design of the Privacy Engine (PE) supports ensuring that data subjects' preferences are adhered to before data is shared (potentially for analytics), and assisting clients of the PAPAYA platform in fulfilling data subject requests related to, e.g., intervenability.

In D3.4, several user interfaces have been developed in order to:

- present risk management artefacts for assessing the privacy risks of privacy-preserving data analytics. This resulted on the enhancement of the current CNIL's PIA too;
- explain and illustrate PAPAYA's WP3 privacy preserving data analytics modules such as privacy preserving Neural Network classification or privacy preserving collaborative training using different privacy enhancing technologies including homomorphic encryption, multi-party computation and differential privacy;
- enhance data subjects' control on their personal data through the Privacy Preference Manager and Data Sunejcts' Right Manager of the Privacy Engine.

2.5 Design and development of an integrated platform (O4)

The complete specification of the PAPAYA platform and the integration of individual PAPAYA modules are described in deliverables D4.2 and D4.3. As a reminder, the PAPAY framework includes:

- the privacy-preserving analytics modules specified in deliverables D3.1 and D3.3;
- the security and transparency services, including the identity access management (IAM) for authentication and authorization services, the auditing service, and the key manager;
- two dashboards for configuration and visualization, namely the platform dashboard for configuration and monitoring purposes and the agent dashboard for agent configuration and visualization of logs;
- a data subject dashboard which integrates one or more tools from the Data subject toolbox namely the tool explaining Privacy-preserving Analytics, Data Disclosure Visualization tool, the Annotated Log View tool and the Privacy Engine.

2.6 End-to-end analysis (O5)

As already mentioned in the first review progress report, the end-to-end analysis will be mainly conducted as part of the work in WP5 (Platform Validation) that will start at M24. The goal of this work package is to set up prototypes demonstrating the five use cases identified in WP2 and validating the requirements listed in deliverable D2.2. Another objective is to produce a platform guide that would help users easily operate the platform.

2.7 Dissemination and Exploitation of the project outcome (O6)

There have been eight publications (articles, posters) in different refereed venues. Some exploitation efforts have been undertaken by means of publications and synergies with other ongoing European H2020 projects such as Poseid-On, Defend, or FutureTPM. The complete list of dissemination and communication activities has moreover been given in deliverable D6.3.

The business plan and exploitation strategy of consortium members have been presented in deliverable D6.4. Potential customers are identified following the key features of the project such

as, the actual privacy preserving data analytics modules, the underlying privacy enhancing technologies, the different use cases and corresponding settings, GDPR compliance aspects, the data subject toolbox, etc. The exploitation strategy for each identified PAPAYA asset (see section 3) has also been defined for the whole consortium and for each partner. Finally, industrial partners have started to work on their business plan.

3 Innovation

Innovation management in the PAPAYA project has been done with the purpose of monitoring the innovation status of activities and check iteratively that the produced outcome is in line with the market expectations.

In the following, we introduce the methodology used to monitor the outcome of the activities and we provide a brief presentation of its results.

3.1 Methodology

3.1.1 Selecting materials and tools

The innovation strategy selected at the beginning of the project (as reported in past deliverables, e.g., D1.2 and D1.3) takes into account three different dimensions:

- the technical dimension, that considers how services in PAPAYA are progressing;
- the organizational dimension, that considers how companies in the consortium are evolving;
- the market dimension, that considers which assets can be brought to the market.

In order to help partners in the consortium keep an eye on these three dimensions, we were prompted to use a specific questionnaire made available by the European Commission, i.e.:

"Marketability assessment of exploitable outputs of REA's H2020 projects (Input from innovation promoter)"

This questionnaire guides each subject in filling in aspects regarding: i) description of the identified assets; ii) detection of relevant sectors for the identified assets; iii) exploitation strategies; iv) market characteristics; v) validation strategy needed to bring the assets to the market; vi) technology transfer from/to subjects that are either internal or external to the consortium; vii) patents and standards that could be generated from the identified assets.

3.1.2 Administering the questionnaires

The selected questionnaires were distributed to partners in the consortium during two different rounds.

Monitoring at M12. During this monitoring period, the consortium identified eight assets that could be subject to marketability (date of submission: January 17th, 2019). However, as these assets were not well divided according to Intellectual Property Rights (IPR) and functionalities, the consortium was further guided in the redefinition of the aforementioned assets, with a second round of questionnaires, with specific instructions such as taking into account IPR as well as competencies of partners. As a result, the number of identified assets at M12 was updated to ten assets (date of submission: July 10th, 2019).

Monitoring at M24. After approximately one year since the first questionnaires' submission, the consortium was asked to revise these, so as to check if the knowledge acquired with the project's progress, the more advanced state of development and a greater understanding of the liaisons between partners could change some of the answers provided at M12. This was indeed the case: However, the number of assets did not change, their descriptions and formulation did, bringing to a more mature view on the available assets (date of submission: March 17th, 2020).

3.2 Results

In this section, we present the results obtained with the M12 and M24 rounds of questionnaires.

3.2.1 Identified assets

In this section, we present the identified assets, as updated during the round of questionnaires at M24. To have a view of the assets recognized at M12, please refer to Deliverable D6.4.

During this round of questionnaires, some asset descriptions were reviewed, to better reflect the current understanding, both in relation with the overall work done in the project and the positioning of such assets with respect to the market.

The following table (Table 1) summarizes the identified assets (and related descriptions), divided in five categories:

- the platform itself;
- the modules devised to privacy-preserving (PP) computation;
- the modules devised to compliance;
- the modules related to eHealth use cases;
- the modules related to Mobile and phone usage use cases.

Table 1 PAPAYA Innovation Assets at M24

Category	Asset	Description
Platform	**Platform for pp Analytics**	The platform will provide to data controllers ability to train and run Machine Learning models (also in collaborative manner) without revealing their private data to the platform and to each other. The product will include two services: (1) Privacy Preserving classification on Neural Network; and (2) Privacy preserving collaborative training of Neural Network
PP Computation	**PP data analytics modules**	The modules ensure the processing of data while being protected. The processing operations can be

		Neural Network classification or trajectory clustering
	PP arrhythmia classifier	This solution aims at classifying arrhythmia disease based on ECG heartbeats in a privacy preserving manner
Compliance modules	**Compliance toolbox**	The Compliance Toolbox consists of a number of software tools that ease legal compliance for organisations using privacy-preserving analytics with the GDPR and related privacy and data protection legislation. The tools focus on the rights of natural persons whose personal data is being processed as part of analytics (i.e., data subjects in the GDPR). Each tool in the toolbox is independent and designed with ease of integration in mind.
	Privacy engine	The Privacy Engine provides to the data subject mechanisms to capture his/her privacy preferences on the collection / use of their personal and/or special categories of personal data for processing in privacy-preserving big data analytics tasks. For that purpose, the Privacy Engine transforms high-level descriptions to computer-oriented policies, allowing their enforcement in subsequent processes to only permit the process of the data that the data subject agrees with e.g. filtering and excluding certain personal attributes. In addition the PE provides to the data subject the mechanism to exercise his/her rights derivative from the GDPR (e.g. the right to erasure his/her personal data). In order to do so, the PE, allows, on one hand, to the data controller to chose the communication channel to obtain the subject desire (email, publisher/subscriber pattern, protection orchestrator), and on the other hand provides a user centric GUI to easily exercise his/her rights.
eHealth use cases	**Stress management**	E-health stress management is a service designed for privacy-compliant detection and mitigation of stress-induced anomalies in workers, coming with a device able to collect physiological measures and linked to a mobile app. Whenever the service identifies a stress condition, it suggests a proper action based on psychologists hints.
	Arrhythmia detection	This tool allows an untrusted party to perform the analysis of a person's ECG signal in a privacy-

		preserving way, leveraging secure platforms such as the PAPAYA one. The tool improves the current MCI software for the analysis of arrhythmias, where a doctor is provided with an ECG signal and looks manually for arrhythmias. The integration with PAPAYA allows the outsourcing of ECG signals for the improvement of analysis performance, while still guaranteeing the preservation of patients' privacy and the protection of data**.**
Mobile And phone usage use cases	**Anonym-TRIP tool**	The tool is composed of two subparts: - Privacy-preserving statistics on traffic measurement - Privacy-preserving trajectory clustering Those two services rely on a combination of analytics operations with PETs mechanisms.
	PP statistics on mobile usage	This service enables third parties to compile statistics on individual use of mobile applications in a privacy preserving manner for each user and provide each user with overall statistics so that he can situate himself in the overall picture. The service is based on a combination of PETs and statistics operations.
	Threat detection for sensitive data	This tool detects deviations from normal behaviour in IT systems (leveraging machine learning techniques for anomaly detection), preserving the confidentiality of the data used in training (that are coming from multiple sources) and/or prediction.

3.2.2 Technology transfer between partners in the consortium

Figure 1 shows the relationships between assets identified at M12.

At this stage, which was quite early considering the overall status of development during the project, some of the relationships between components (represented with arrows in Figure 1) were already recognizable: partners succeeded in understanding which kind of technology transfer (between consortium partners) was needed to ensure a proper marketability of their assets. However, at this stage, the role played by specific assets (e.g., the Compliance toolbox) with respect to all the other assets was still unclear (and this is why Figure 1 lacks some arrows).

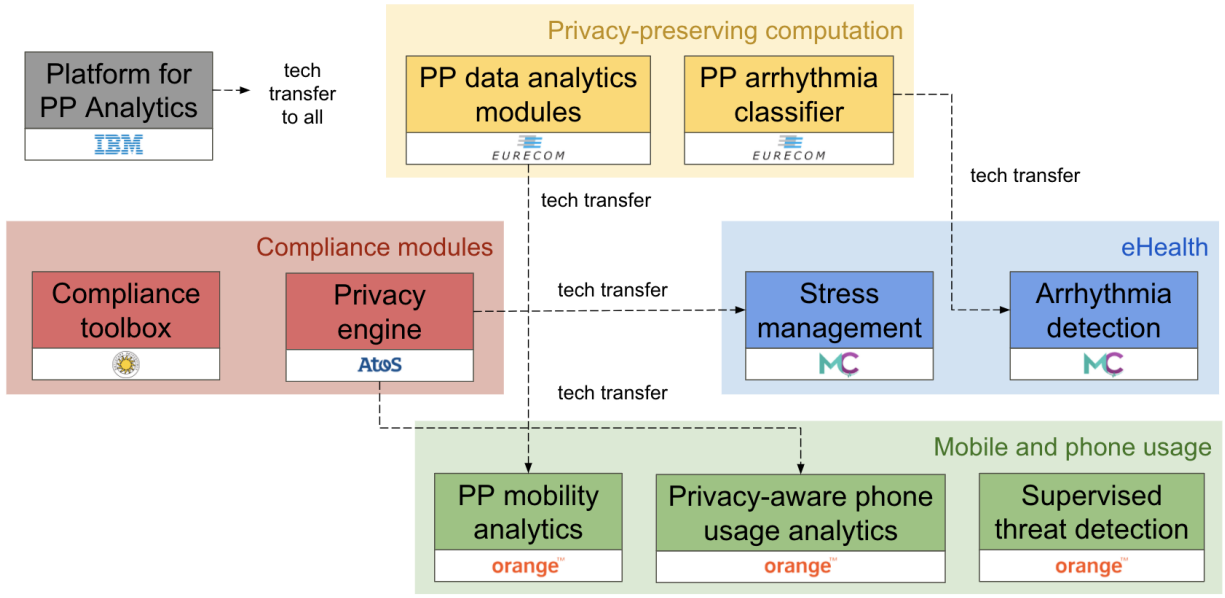

Figure 1 Assets identified at M12

Figure 2 shows an update of Figure 1, resulting from the round of questionnaires performed at M24.

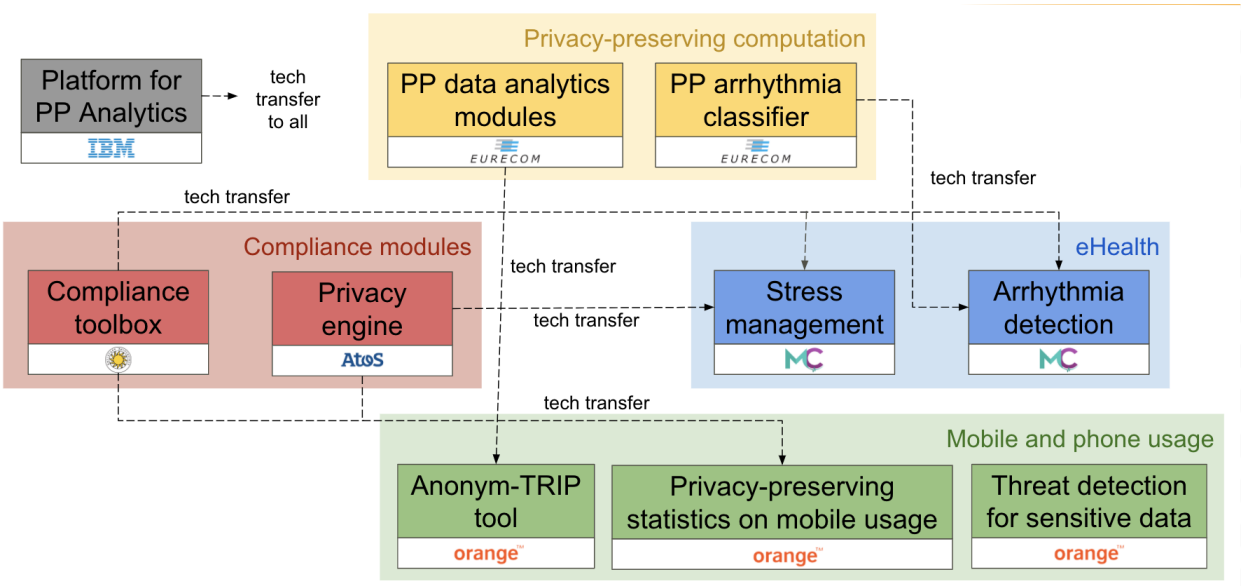

Figure 2 Assets identified at M24

Though the number of assets did not change, some relationships between assets (i.e., technology transfer needed to make the end-to-end solution work) were redefined/added (together with some

redefinition of details, e.g., asset names, in compliance with what shown in Section 3.2.1). We believe that the picture emerging from this round of questionnaires is valuable, as, taken each asset, it is clear now what other assets are needed (in technology transfer) to propose them to the market as a standalone solution, either as a component to build something bigger (like in the case of privacy-preserving computation modules or compliance modules) or as an end-to-end solution (like in the case of use cases).

3.2.3 Relevant sectors

Figure 3 shows how the perception of relevant sectors changed between the two rounds of questionnaires:

- at first, the sectors recognized as favorable for the marketability of assets were: Knowledge and Digital Economy, Social infrastructure and Transport;
- after the second monitoring, two additional sectors were recognized as favorable: Resources and environment (Privacy-preserving statistics on mobile usage) and Financing for SMEs (Threat detection for sensitive data).

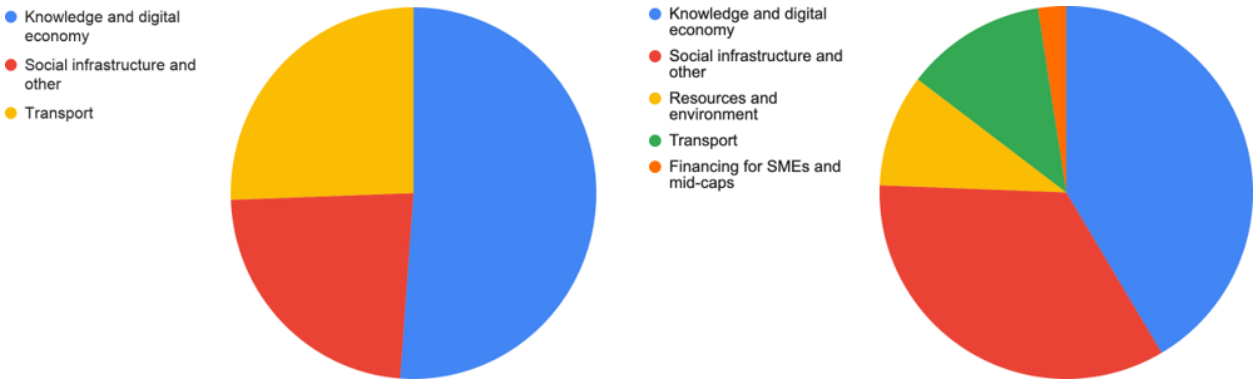

Figure 3 Relevant sectors for the identified assets (left: M12; right: M24)

3.2.4 Exploitation strategy

Figure 4 shows how the perception of potential exploitation assets was changed between M12 and M24. More specifically:

- The description of one component from the Mobile and phone usage category (the Mobile usage statistic tool component in Deliverable D6.4) from M12 and M24, and with that, its exploitation strategy is also updated, removing the possibility of being licensed to a third party and of being used within an internal process creating benefits for the company;
- Similarly, the description and exploitation strategy of another component (the Threat detection for sensitive data tool mentioned in Deliverable D6.4) were changed. It is now indicated as scientific exploitation;

- Due to new market possibilities (specifically for the Stress management component), we count a new product indicated as a potentially new product.

Figure 4 Exploitation strategy for the identified assets (left: M12; right: M24)

Figure 5 shows that a better understanding of the proposed assets, as a result of a more profound work of development in the project, brought the consortium to a better understanding of the time needed to go to the market. The results show that most of the assets are presumably going to be ready in the lifespan of PAPAYA, while the less mature are going to take more than 3 years to be ready.

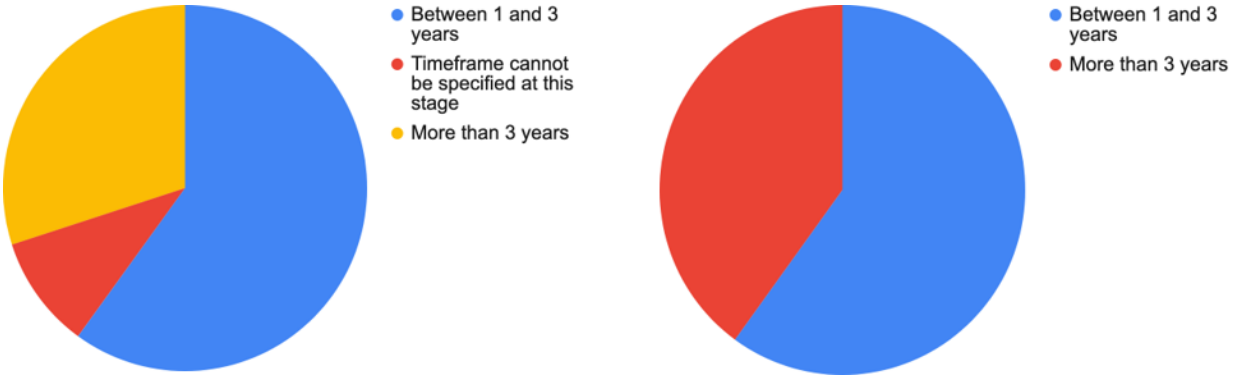

Figure 5 Time to market (left: M12; right: M24)

Figure 6 shows the understanding the consortium had about the needed validation strategy at M12. It is clear that, due to the immaturity of the development and a lack of understanding of the relationships between components, the validation strategy that were considered as more difficult to achieve (e.g., the ones related to real-world validation) were tagged as “not needed” although “desirable”.

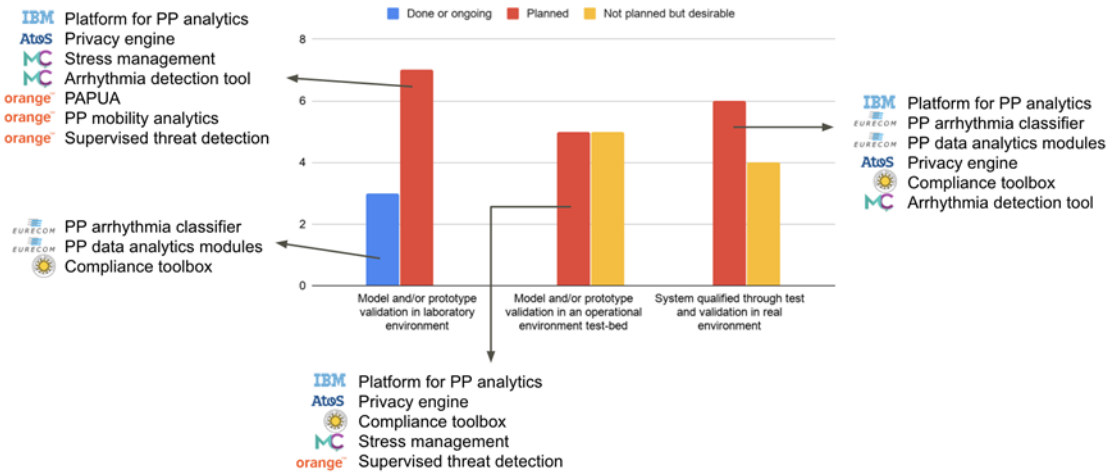

Figure 6 Validation strategy at M12

However, as time progressed, the maturity of the development of PAPAYA assets opened new validation scenarios. Figure 7 shows the validation strategy proposed at M24. When compared with Figure 6, Figure 7 shows a shift of columns to the left (i.e., from "not planned" to "planned" and from "planned" to "done or ongoing"), showing that validation has started at least for some validation categories (e.g., in laboratory) and that some new possibilities for validation will be considered during the course of the project.

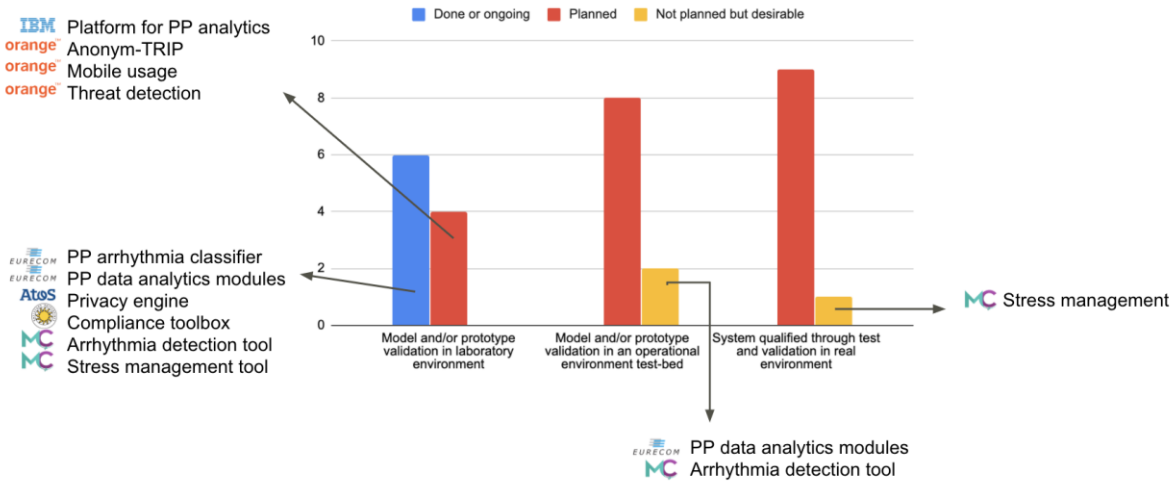

Figure 7 Validation strategy at M24

3.2.5 Technology transfer to/from third parties outside the project

Figure 8 shows the expected technology transfer to/from third parties outside the project at M12. At this stage, all identified assets were not expected to use components from outside the project. Moreover, just a small set of the identified assets (three of them coming from an academic environment) was presumably interested in a possible transferring outside the project (i.e., to allow something from outside the project to use their outcomes with a technology transfer kind of relationship).

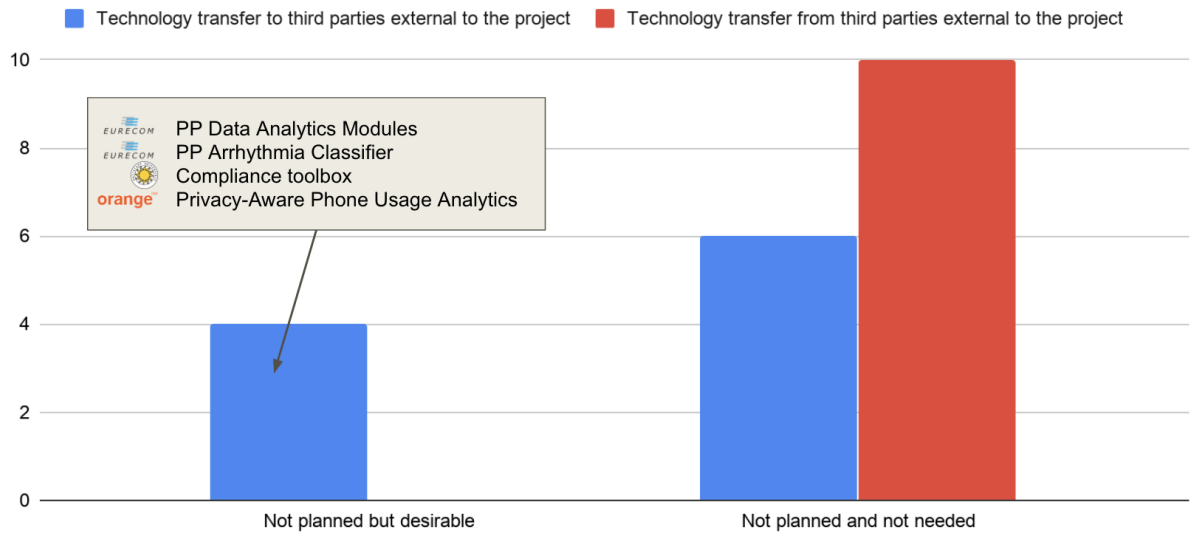

Figure 8 Technology transfer to/from outside the project, at M12

Figure 9, instead, provides an updated view, at M24. Here, a component (out of 10) opens to the possibility of using components from outside the project consortium for its development, while more components with respect to the ones at M12 open to the possibility of being reused outside the project consortium.

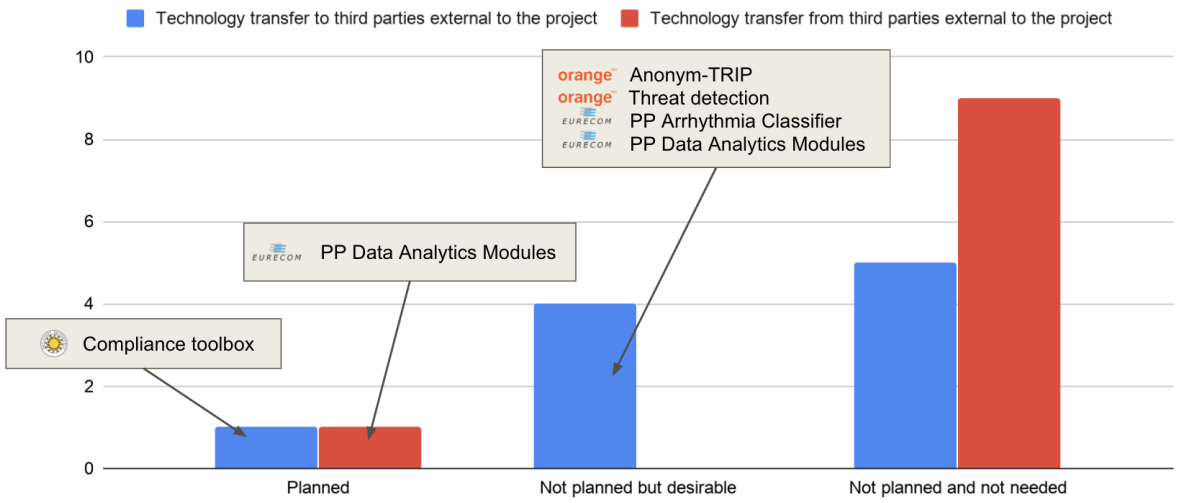

Figure 9 Technology transfer to/from outside the project, at M24

3.2.6 Patents and standards

In the following table (Table 2), we present the expected patents and standards, as an outcome of the questionnaires at M24.

Table 2 PAPAYA potential patents and standards

Component	Application type	Subject of application
Platform for PP Analytics	**Patent**	The platform itself
Stress management tool	**Patent**	Stress detection algorithm
Anonym-TRIP tool	**Patent**	Trajectory clustering in the encrypted domain
Compliance Toolbox	**Creation of a new standard**	Standards on DPIA
Stress management tool	**Compliance with existing Quality standards**	ISO 13485
Arrhythmia detection tool	**Compliance with existing Quality standards**	ISO 13485

4 Dissemination, Communication and Exploitation Activities

4.1 Scientific Publications

We report in this section, the scientific publications we have obtained since the beginning of the project.

Publication #1

Type of scientific publication	article
Title of scientific publication	FHE-compatible Batch Normalization for Privacy Preserving Deep Learning
DOI	https://doi.org/10.1007/978-3-030-00305-0_27
ISSN or eSSN	
Authors	Alberto Ibarrondo, Melek Önen
Title of journal or equivalent	International Workshop on Data Privacy Management
Number, date	
Publisher	Springer
Place of publication	
Year of publication	2018
Relevant pages	pp 389-404
Peer-review	yes
Is/Will open access provided to this publication	yes

Publication #2

Type of scientific publication	extended abstract & poster
Title of scientific publication	A Hybrid Protocol for Private Neural Network Predictions
DOI	http://www.eurecom.fr/fr/publication/5955/download/sec-publi-5955_1.pdf
ISSN or eSSN	
Authors	Gamze Tillem, Beyza Bozdemir, Melek Önen
Title of journal or equivalent	8th edition of ICT.OPEN
Number, date	
Publisher	

Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	
Is/Will open access provided to this publication	Yes

Publication #3

Type of scientific publication	article
Title of scientific publication	PAPAYA: A platform for Privacy Preserving Data analytics
DOI	https://ercim-news.ercim.eu/en118/special/papaya-a-platform-for-privacy-preserving-data-analytics
ISSN or eSSN	
Authors	Eleonora Ciceri, Marco Mosconi, Melek Önen and Orhan Ermis
Title of journal or equivalent	ERCIM News Magazine
Number, date	ERCIM News 118, Special Theme
Publisher	ERCIM
Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	No
Is/Will open access provided to this publication	Yes

Publication #4

Type of scientific publication	poster
Title of scientific publication	Privacy Preserving Neural Network Classification
DOI	
ISSN or eSSN	
Authors	Gamze Tillem, Beyza Bozdemir, Melek Önen and Orhan Ermis
Title of journal or equivalent	PUT 2019, Open Day for Privacy, Usability, and Transparency
Number, date	

Publisher	
Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	Yes
Is/Will open access provided to this publication	Yes

Publication #5

Type of scientific publication	article
Title of scientific publication	SoK: Cryptography for Neural Networks
DOI	https://doi.org/10.1007/978-3-030-42504-3
ISSN or eSSN	
Authors	Monir Azraoui, Muhammad Bahram, Beyza Bozdemir,Sébastien Canard, Eleonora Ciceri, Orhan Ermis, Ramy Masalha, Marco Mosconi, Melek ̈Onen, Marie Paindavoine, Boris Rozenberg, Bastien Vialla,and Sauro Vicini
Title of journal or equivalent	Privacy and Identity Management. Data for Better Living: AI and Privacy
Number, date	14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School
Publisher	Springer
Place of publication	
Year of publication	2019
Relevant pages	pp. 63-81
Peer-review	Yes
Is/Will open access provided to this publication	Yes

Publication #6

Type of scientific publication	article
Title of scientific publication	Interactive Focus Group GDPR-compliant Dynamic Consent Management
DOI	

ISSN or eSSN	
Authors	E. Schlehahn, S. Fischer-Hübner, R. Wenning, M. Patrick, F. Karegar
Title of journal or equivalent	Privacy and Identity Management. Data for Better Living: AI and Privacy
Number, date	14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School
Publisher	Springer
Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	Yes
Is/Will open access provided to this publication	Yes

Publication #7

Type of scientific publication	article
Title of scientific publication	Protecting different interests in big data analytics - Current trends and solutions
DOI	
ISSN or eSSN	
Authors	Tjerk Timan, Zoltan Mann, Rosa Araujo, Alberto Crespo Garcia, Ariel Farkash, Antoine Garnier, Akrivi Vivian Kiousi, Paul Koster, Antonio Kung, Giovanni Livraga, Roberto Díaz Morales, Melek Önen, Ángel Palomares, Angel Navia Vázquez, Andreas Metzger
Title of journal or equivalent	Big Data Value Association
Number, date	
Publisher	
Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	No
Is/Will open access provided to this publication	Yes

Project No. 786767

Publication #8

Type of scientific publication	article
Title of scientific publication	PAC: Privacy-preserving Arrhythmia Classification with neural networks
DOI	http://www.eurecom.fr/fr/publication/6046
ISSN or eSSN	
Authors	Mohamad Mansouri, Beyza Bozdemir, Melek Önen, Orhan Ermis
Title of journal or equivalent	FPS 2019, 12th International Symposium on Foundations and Practice of Security
Number, date	
Publisher	Springer
Place of publication	
Year of publication	2019
Relevant pages	
Peer-review	Yes
Is/Will open access provided to this publication	Yes

4.2 Conferences, workshops and other events

4.2.1 Scientific conferences, workshops

Participation.

- Technical/scientific presentations, business presentations, presentations to the public, etc.
- Prize for MCI in Harmonic Innovation 2019.
- EURC obtained one best poster and one best paper award.
- IBM presented the technologies being developed in PAPAYA to Israeli Population and Immigration authority in August 2019.
- Simone Fischer-Hübner (KAU) has given a PAPAYA overview presentation at PUT 2019, and presentation requirement elicitation work at the ENISA/ULD workshop, the CyberSec4Europe panel, and the NECS winter school 2020 (see details in Table 3).

Organization.

Privacy and Security technologies at IBM Haifa: event hosting (IBM), presentation on privacy-preserving training of neural network

Special track on privacy, security and informed consent in healthcare at CBMS 2019: organization (KAU), members of the program committee (KAU, EURC, ORA)

Open day for Privacy, Usability and Transparency (PUT 2019), co-located with PETS 2019 conference: organization with PRIVACY&US and SPECIAL EU projects, workshop chair (EURC, KAU), PAPAYA presentation (KAU)n, poster presentation (EURC)

IFIP Summer School 2019 on Privacy and Identity Management and related workshops: chair (EURC), member of the Steering Committee (KAU), technical sponsor, 2 parallel workshops organization (with SPECIAL on one side, and with PoseID-on on the other side).

Table 3 provides an overview of all the events attended by PAPAYA members.

Table 3 Events attended by PAPAYA

Name of Event	Date	Place	Partner	Audience	Comment
Forum 5i	May 15, 2019	Grenoble, France	ORA	Industrials	Participation and presentation of privacy preserving NN demo on arrhythmia
Workshop on privacy, data protection and digital identity	July 11, 2019	Coimbra, Portugal	EURC	Technical audience	Presentation of an overview of the PAPAYA project
PUT 2019 workshop, collocated with PETS 2019	July 15, 2019	Stockholm	KAU	Technical & Legal Audience	Short Overview presentation about PAPAYA
IFIP Summer School on Privacy and Identity Management	August 19, 2019	Brugg, Switzerland	EURC	Technical audience	Representation of PAPAYA project and participation as one of the PC-chairs
Workshop "Pseudonymization and relevant security techniques", jointly organised by ULD and ENISA	November 12, 2019	Berlin, Germany	KAU	Technical, Social Science & Legal audience	Presentation on Choices and Challenges of Implementation & Configuration, also briefly reporting about PAPAYA
Panel participation at the CyberSec4Europe concertation event	November 14, 2019	Toulouse, France	KAU	Technical, Social Science, Legal audience (from H2020 Cyber Security pilots)	Panel presentation on Challenges of User-Centric Privacy Preserving IDM , also mentioning work in PAPAYA

Workshop on Cyber-Security Arms Race (CYSARM)	November 15, 2019	London, UK	EURC, ORA	Technical audience	Co-organization of the workshop with FutureTPM, Astrid and PROMETHEUS projects
NECS Winter School 2020	January 14, 2020	Trento, Italy	KAU	Technical audience	2-hours lecture on Usable Privacy, presenting also work in PAPAYA WP2.
Semestre thématique Cybersécurité du Labex CIMI	January 22, 2020	Toulouse, France	EURC	Technical audience, Industrials	Presentation on the topic of data privacy and AI (with an overview of PAPAYA)
EURECOM's scientific council	February 7, 2020	Sophia-Antipolis, France	EURC	Technical audience, Industrials	Demonstration of the privacy preserving arrhythmia detection
Meetup ClusterIA	February 20, 2020	Sophia-Antipolis, France	EURC	Technical audience, Industrials	Presentation of research and innovation on privacy preserving AI (with an overview of PAPAYA)
Online workshop on Privacy Labelling organised by Oslo University	March 12, 2020	Online	KAU	Interdisciplinary	Presentation on "Privacy Labelling in larger Perspective", also reporting about trust requirements elicited in WP2.

4.3 Collaboration with other research projects

We have several collaborations with other research projects. Such interactions are related to exchange of knowledge and technologies with some projects related to privacy and cryptography, and also some common communications activities.

More precisely, we can list the following projects, with related topics:

- PoseID-on on privacy dashboard, PP NN
- DEFeND on the CNIL PIA tool development
- FutureTPM and PROMETHEUS on cryptography
- Privacy&Us, Cybersec4Europe, SPECIAL, GDPR Cluster Projects, KRAKEN and TRUSTEE on security and privacy.
- CyberSec4Europe on the elicitation of end user requirements.

Those collaborations are necessary to establish synergies with current actions and to maximize the impact of PAPAYA's dissemination activities.

4.4 Web presence

As part of the project outreach activities, PAPAYA´s team has established and developed the web presence via the project website[1] and social networking platforms such as Twitter[2] and LinkedIn[3]. While the website gives general information about the project, its objectives, the technical approach and the involved partners, we resort to the social platform to regularly report the key steps of the project, update, inform the main dissemination and communication activities, and create a community of followers.

4.4.1 PAPAYA website

The PAPAYA website has been launched on August 6th, 2018 (M4) and is maintained by ATOS. Deliverable D6.1, produced at M3, consists and describes its structure, design, and the technical details of the website. Additionally, the latest dissemination and communication report produced for M18 (D6.2) included the full analytics results provided by Google. All PAPAYA partners contribute and collaborate with the sharing of relevant content to be published on the website. At the time of writing this report, the "News" section is the most active page of the website (see figure 10). At the same time, our team continuously updates the "Dissemination" section with the newly released material and actualize the "Related Projects" part with the new collaborative projects.

[1] PAPAYA website: https://www.papaya-project.eu/
[2] Twitter profile: https://twitter.com/ProjectPapaya
[3] LinkedIn profile: https://www.linkedin.com/company/papaya-project-eu-h2020

Figure 10 PAPAYA website

The main figures related to the website statistics are presented in Table 4. We can observe the number of unique sessions (i.e. the interactions a user takes within a given period) triggered by the visitors is 2,169 with an average session duration of 2 minutes, approximately. 88% of these users have visited the website for the first time. Given this number, we have to take into consideration the fact that Google Analytics identifies a “new user”, on the one hand, with an existing tracking cookie on their device, and, if there is no tracking cookie, then Google creates one and considers this as a "new visitor" for our website; on the other hand, if there is an existing tracking cookie on some devices, then the service is counting this user as a "returning visitor".

These metrics provide us much valuable information and help to see how we could increase the website presence and visibility or which sources have to be improved such as some traffic channels. Nevertheless, the main results included in the rows illustrate the acceptable performance of the website

Table 4 PAPAYA Web Statistics

	M12-M24 (March 23rd, 2020)	Target Y2
Sessions	2,169	2000
Users	1,585	1500
Average Session Duration	02:06	2:00
New visitors	88%	85%

4.4.2 PAPAYA Twitter

The PAPAYA Twitter account has been created in June 2018 (M2) and is maintained by ORA. All PAPAYA partners contribute to the provision of relevant content to be published on Twitter. A Twitter account is one of the key social media tools which give PAPAYA the opportunity to effectively communicate and disseminate the relevant updates and results throughout real-time messages. In the current report, we include the numbers of our activities from M12 to M24. As shown in Table 5, we did not fully reach one of the objectives we set in D6.3 for Y2 in terms of the number of followers; At the same time, the number of tweets is acceptable and also the total number of followers and tweets for 2 years remains high.

Table 5 Twitter statistics

	M12-M24	Target Y2
Number of Followers	64	100
Number of Tweets	51	50

Figure 11 PAPAYA Twitter Account

4.4.3 PAPAYA LinkedIn

The PAPAYA LinkedIn company page is alive since June 2018 (M2) and is maintained by ORA. All PAPAYA partners contribute to the provision of relevant content to be published on LinkedIn. LinkedIn is a more professional social networking tool and in the same way as Twitter helps us to post and share information related to the project in a professional and online environment. The following report includes the numbers of our activities from M12 to M24.Table 6 shows that we did not fully attain the objectives set for Y2 in terms of the number of followers and the number of updates (the posts that are published on a LinkedIn page). We believe that there will be a considerable rise at Y3 as the LinkedIn audience is more technical and commercial than Twitter, and as soon as PAPAYA results are available, LinkedIn will be a perfect channel for dissemination and for reaching the targeted stakeholders.

Table 6 LinkedIn statistics

	M12-M24	Target Y2
Number of Followers	18	50
Number of Updates	18	20

Figure 12 PAPAYA Linkedun Adin Account

5 Progress Overview at each WP

This section describes the activities of each partner on a per Work Package, per Task basis. For the sake of clarity, the tables depicting the resources per partner and per Task for each WP correspond to the M17-M24 period since the previous EC1 report corresponds to M1-M16.

5.1 Work Package 1: Project Management

WP Leader: EURC

Contributors: All partners.

5.1.1 Progress towards the objectives

This work package aims at coordinating project management activities through regular monitoring of the work carried out at each work package and following the allocated budget. During the second year of the project, we had our first review meeting towards the end of M18. We prepared the related reports. Based on the feedback of our reviewers, we have also prepared a report on the clarification of end-users of each component of the PAPAYA platform. Furthermore, our GA meeting planned on February 25th and 26th in Trento was cancelled due to the Covid-19 pandemia and was replaced by a 2-day remote meeting. Finally, the current deliverable reports on the Y2 activities.

5.1.2 Deviations

No deviations are detected during this period.

5.1.3 Task 1.1: Project Management and Reporting

Task Leader	EURC
Contributors	All
Overall task progress	The task is progressing successfully as planned. Due to the Covid-19 pandemia, we had to cancel our physical GA meeting in Trento and replaced it with a 2-day remote meeting (through webex). The relevant costs are summarized in Appendix 1 and will be submitted to the EC portal. D1.4 (the current one) is submitted on time.
Work carried out by beneficiaries (M13-M16)	**EURC**: EURC has monitored the activities for the first review meeting. **KAU**: KAU contributed with the required reporting. **MCI**: MCI contributed with the required reporting. **ORA**: Participation to conf calls and organization of the review meeting. **ATOS**: Reporting the effort in the associated reports.

Work carried out by beneficiaries (M17-M24)	**EURC**: EURC started to prepare the second review meeting. EURC also monitored the preparation of the additional document on end-users for PAPAYA components as requested from the review report. Finally, EURC is editing D1.4. **IBM**: Preparation and participation to the review meeting **KAU**: KAU contributed with the required reporting, participation to the review meeting. **MCI**: Support during management aspects and reporting steps **ORA**: Preparation and participation to the review meeting. **ATOS**: Reporting effort and participation to the review meeting

5.1.4 Task 1.2: Quality Assurance and Risk Management

Task Leader	EURC
Contributors	All
Overall task progress	The task is progressing successfully as planned. All WP leaders are monitoring the work in their corresponding WPs. Partners also have participated to the internal reviewing of deliverables. WP5 has started at M24.
Work carried out by beneficiaries (M13-M16)	**EURC**: EURC monitored the production of M15 deliverables.
Work carried out by beneficiaries (M17-M24)	**EURC**: monitored the production of Y2 deliverables. **MCI**: Support in quality assurance.

5.1.5 Task 1.3: Innovation Management

Task Leader	MCI
Contributors	MCI, EURC
Overall task progress	The task is progressing as planned. The innovation questionnaire has been updated and this second version has been submitted to the EC portal. This report (see Section 3) reports the results monitored through the selected questionnaires at month M12 and month M24.
Work carried out by beneficiaries (M13-M16)	**MCI**: MCI prepared the innovation slot for the review meeting. **ORA**: Participation to the redaction of a new version for questionnaires related to marketability.
Work carried out by beneficiaries (M17-M24)	**EURC**: EURC contributed to the new version of the innovation questionnaire **IBM**: Contribution to the innovation management activities

	MCI: Following the first review of the PAPAYA project, MCI supported the preparation, summarisation and submission phases of the innovation questionnaires (due to M24) **ORA**: Redaction of the new version of the innovation questionnaire for Orange.

5.1.6 Meetings/calls in WP1

Date	Location	Reason
16 May 2019	Conference call	EURC, IBM, MCI, ORA, EC meeting on innovation questionnaires
19 May 2019	Conference call	Innovation- Exploitation call
29 May 2019	Conference call	Innovation- Exploitation call
4 September 2019	Conference call	Review agenda meeting
3 October 2019	Conference call	Review preparation meeting #1
22 October 2019	Conference call	Review preparation meeting #2
28 October 2019	Brussels	Preparation of the first project review
29 October 2019	Brussels	First project review meeting
6 November 2019	Conference call	ATOS-EURC, meeting on innovation aspects
10 December 2019	Conference call	Meeting on review feedback
8 January 2020	Conference call	Meeting on responses to reviewers
26 February 2020	Conference call	WP1 slot at the remote GA meeting

5.2 Work Package 3: Privacy Enhancing Technologies for Data Analytics

WP Leader: EURC

Contributors: ATOS, EURC, IBM, KAU, ORA

5.2.1 Progress towards the objectives

All partners finalized the specification of the privacy preserving PAPAYA modules (Neural Network classification, collaborative NN training, trajectory clustering, basic statistics), the user interfaces and the Privacy Engine. Deliverables D3.3 and D3.4 report on these activities. This WP has ended at M24.

5.2.2 Deviations

As mentioned in the previous deliverable, the use case designer for UC1 and UC2 in the healthcare umbrella, MCI has also contributed to the specification of privacy preserving data analytics in particular for Neural Network classification and collaborative training.

ATOS has developed the user interfaces (server sides and mobile apps) for the integration of the Privacy Engine within the PAPAYA framework, which were not contemplated within the initial description of actions.

5.2.3 Task 3.1: Single-Owner privacy preserving data analytics

Task Leader	EURC
Contributors	EURC, IBM, ORA
Overall task progress	EURC, IBM and ORA have developed their solution on privacy preserving Neural Networks. MCI supported the implementation of the privacy preserving arrhythmia detection tool. This task can be considered as successfully ended at M24.
Work carried out by beneficiaries (M13-M16)	**EURC**: EURC has implemented a PoC for Swann (PHE based NN) and evaluated its performance. **IBM**: Generic implementation and evaluation of hybrid approach for pp classification **MCI** supported for the implementation of pp arrhythmia detection. **ORA**: Work on new benchmarks for our FHE based ECG analysis in order to compare the different results obtained by the consortium.
Work carried out by beneficiaries (M17-M24)	**EURC**: EURC has implemented and evaluated the 2PC based pp arrhythmia detection solution. These are reported in D3.3. **IBM**: Finalize implementation and evaluation of hybrid approach for PP classification; design, implementation and evaluation of a method for PP training of NN **MCI**: MCI supported the partners involved in the technical specification of algorithms and techniques for what concerns UC1, i.e., the arrhythmia detection pilot **ORA**: Modification of the FHE based neural network inference to suit Orange use case on threat detection. Management and redaction of deliverable D3.3.

5.2.4 Task 3.2: Multi sources privacy preserving data analytics

Task Leader	ORA
Contributors	EURC, IBM, ORA, MCI
Overall task progress	EURC, IBM, and ORA manly contributed to the specification of the PAPAYA modules investigated in T3.2 (collaborative training, clustering, statistics). MCI

	contributed to the specification of the privacy preserving Neural Network collaborative training solutions. This task can be considered as successfully ended at M24.
Work carried out by beneficiaries (M13-M16)	**EURC**: The design of the 2-server based privacy preserving NN classification is finalized. The development has started. **IBM**: Generic implementation of a Shmatikov based approach for PP collaborative training of DNN. **MCI**: MCI supported the partners involved in the technical specification of algorithms and techniques for what concerns UC2, i.e., the stress management pilot. **ORA**: Work with EURC to compare different trajectory clusterings. Work on encrypted Bloom filters by comparing cryptographic approaches. Work on the functional encryption scheme sued for mobile stat use case. Work on neural network for threat analysis.
Work carried out by beneficiaries (M17-M24)	**EURC**: EURC has worked together with ORA on the trajectory clustering algorithm and propose the design of a server aided privacy preserving variant of TRACLUS. **IBM**: Evaluation of Shamtikov based approach for PP collaborative training on ECG data. Implementation and evaluation of a Abadi based method for PP collaborative training. Research and implementation of property inference attack on PP collaborative training. **MCI**: MCI supported the partners involved in the technical specification of algorithms and techniques for what concerns UC2, i.e., the stress management pilot. **ORA**: Redaction of the specification for encrypted Bloom filters, permitting counting, union and intersection. Work and specification of a new trajectory clustering based on the MinHash algorithm. Exchanges with EURC to compare both approaches.

5.2.5 Task 3.3: Risk Management and Transparency for the data analytics platform

Task Leader	KAU
Contributors	ATOS, EURC, IBM, KAU, ORA
Overall task progress	KAU and ATOS mainly contributed to the development of user interfaces and the privacy engine respectively. ORA and MCI investigated the integration of these components to the use cases. EURC and IBM contributed to this task by evaluating the quality of components developed in T3.1 and T3.2.
Work carried out by beneficiaries (M13-M16)	**KAU**: KAU extended the CNIL PIA tool, which results in an improved visualization of risk management artefacts to be shown to data subjects.
Work carried out by beneficiaries (M17-M24)	**EURC**: EURC has evaluated the accuracy of Swann and the 2PC based privacy preserving arrhythmia detection tool. This does not decrease

	significantly. The quality of ppTRACLUS is evaluated through silhouette analysis. **IBM**: Research, implementation and evaluation of a defence method against property inference attack **KAU**: KAU developed user interfaces (UIs) for explaining privacy risk based on risk analysis artefacts and for explaining privacy-preserving data analytics to data subjects and other stakeholders. KAU contributed with the editorial work and with content contributions to D3.4. **MCI**: MCI followed calls and questions from the technical partners, that concerned user-specific aspects and expected views. **ORA**: Interaction with ATOS and KAU to better understand the Privacy Engine and the Data Subject Tools respectively, so as to be able to integrate those components into Orange prototypes. Internal reviewer of D3.4 on Transparent Privacy-Preserving Data Analytics **ATOS**: Development of the Privacy Engine tools, contributing to the corresponding deliverables associated

5.2.6 Meetings/calls in WP3

Date	Location	Reason
13 May 2019	Conference call	WP3 monthly meeting
15 May 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
5 June 2019	Conference call	WP3 monthly meeting
7 June 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
17 June 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
3 July 2019	Conference call	WP3 monthly meeting
26 July 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
25 July 2019	Conference call	EURC-ORA-IBM-MCI meeting on joint paper
26 July 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
4 September 2019	Conference call	WP3 monthly call
2 October 2019	Conference call	WP3 monthly call
16 October 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
22 November 2019	Conference call	Task 3.4 meeting
4 December 2019	Conference call	WP3 monthly call
11 December 2019	Conference call	EURC-ORA meeting on pp trajectory clustering
8 January 2020	Conference call	WP3 monthly call
5 February 2020	Conference call	WP3 monthly call

14 February 2020	Conference call	EURC-ORA meeting on pp trajectory clustering
25 February 2020	Conference call	WP3 slot during the remote GA meeting
1 April 2020	Conference call	WP3 monthly call

5.3 Work Package 4: Platform Design and Development

WP Leader: IBM

Contributors: ATOS, EURC, KAU, IBM, ORA

5.3.1 Progress towards the objectives

In this reporting period, we (1) finalized the design of the PAPAYA framework, including the Data Subject toolbox and Security and Transparency services; (2) set up the PAPAYA platform; (3) defined deployment and integration evaluation procedures; (4) implemented and deployed several privacy preserving analytic services and the first version of the platform dashboard.

The next steps are: (1) complete the development and the deployment remaining privacy preserving analytic services; (2) complete the development and the deployment of the Data Subject Toolbox; (3) complete the development and the deployment of Security and Transparency services; and (4) finalize the platform dashboard.

5.3.2 Deviations

As for the case of WP3, the use case designer for UC1 and UC2 in the healthcare umbrella, MCI has participated to the discussions related to architecture design and implementation, with a greater effort than what was planned in the DoA, specifically for:

- the activities related to privacy-preserving services on Neural Network classification and collaborative training;
- the activities related to the design of the dashboard (specifically for user-related aspects).

In addition, ATOS is already developing the user interfaces (server sides and mobile apps) for the integration of the Privacy Engine within the PAPAYA framework, which were not contemplated within the initial description of actions.

5.3.3 Task 4.1: Design models and architecture

Task Leader	IBM
Contributors	ATOS, EURC, IBM, KAU, MCI, ORA
Overall task progress	The task is completed

Work carried out by beneficiaries (M13-M16)	**EURC**: Contribution to platform design and D4.1 with respect to pp analytics services **IBM**: overall design of the PAPAYA framework and leading the D4.1 **KAU**: Contribution to platform design with respect to platform dashboards, leading design of Data Subject tool and transparency services **MCI** supported the technical partners in the architecture design offering views and expected behaviours from the point of view of use cases **ORA**: Contribution to platform design and D4.1 with respect to pp analytic services **ATOS**: Contribution to platform design and D4.1 with respect to Data Subject tool, Security related tools/services
Work carried out by beneficiaries (M17-24)	The task is completed

5.3.4 Task 4.2: Development of the platform and integration of PETs

Task Leader	IBM
Contributors	ATOS, EURC, IBM, KAU, MCI, ORA
Overall task progress	The task is progressing well.
Work carried out by beneficiaries (M13-M16)	The task has not started yet
Work carried out by beneficiaries (M17-M24)	**EURC**: Deployment and integration evaluation of pp arrhythmia detection service; start integration of other pp analytic services developed by EURC; contribution to D4.2. **IBM**: Setup PAPAYA framework environment (Kubernetes service); dockerization, deployment and integration evaluation of PP classification and PP Collaborative Training services; leading D4.2. **KAU**: Development of auditing mechanisms; contribution to D4.2. **MCI**: T4.1, MCI supported the technical partners in what concerns the design and implementation of the platform, ensuring that the implementation follows the expected behaviour as for the use cases **ORA**: Development and first tests of the encrypted Bloom filters, and the trajectory clustering on encrypted data; contribution to D4.2. **ATOS**: Developing of the IAM and Key Manager services; contribution to D4.2.

5.3.5 Task 4.3: Dashboard for the platform

Task Leader	KAU
Contributors	ATOS, EURC, IBM, KAU, MCI, ORA
Overall task progress	The task is progressing according to plan with the first version of the platform dashboard deployed and steady progress on the data subject toolbox. Some tools in the toolbox have early versions already implemented
Work carried out by beneficiaries (M13-M16)	**KAU**: work on the design of tools in the data subject toolbox for communicating risks.
Work carried out by beneficiaries (M17-M24)	**IBM**: We implemented and deployed the 1st version of the platform dashboard **KAU**: KAU started with the ongoing implementation of data subject user interfaces as part of the data subject toolbox. **MCI**: MCI offered support to technical partners for what is expected from dashboards, specifically from the point of view of end users. **ORA**: Interaction with partners to better understand the platform dashboard. **ATOS**: Adapting the Privacy Engine tools developed for an easy integration and deployment within the Papaya framework and contributing with the corresponding deliverables.

5.3.6 Meetings/calls in WP4

Date	Location	Reason
13 May 2019	Conference call	WP4 bi-weekly call
27 May 2019	Conference call	WP4 bi-weekly call
24 June 2019	Conference call	WP4 monthly call
2 September 2019	Conference call	WP4 monthly call
9 December 2019	Conference call	WP4 monthly call
6 January 2020	Conference call	WP4 monthly call
3 February 2020	Conference call	WP4 monthly call
13 April 2020	Conference call	WP4 monthly call

5.4 Work Package 5: Platform Validation

WP Leader: MCI

Contributors: ATOS, EURC, KAU, IBM, ORA

5.4.1 Progress towards the objectives

As the activities for this work package have just started, all the effort spent for now is focused on planning a roadmap to coordinate: i) the development in WP4; ii) the integration and validation of use case scenarios in WP5. Some partners already started on the integration of the individual modules.

5.4.2 Deviations

No deviations.

5.4.3 Task 5.1: Validation through e-health UC

Task Leader	MCI
Contributors	ATOS, EURC, IBM, KAU, ORA
Overall task progress	Partners have been jointly working on defining a roadmap of integration and validation.
Work carried out by beneficiaries (M13-M16)	The task has not started yet.
Work carried out by beneficiaries (M17-24)	**MCI**: MCI has been working on preparing a plan for integration and validation

5.4.4 Task 5.2: Validation through web analytics UC

Task Leader	ORA
Contributors	ATOS, EURC, IBM, KAU,
Overall task progress	Partners have been jointly working on defining a roadmap of integration and validation.
Work carried out by beneficiaries (M13-M16)	The task has not started yet
Work carried out by beneficiaries (M17-M24)	**ATOS**: Initial work on the integration of the different tools developed by Atos

5.4.5 Task 5.3: Technology assessment and recommendations

Task Leader	MCI
Contributors	All

Overall task progress	Partners have been jointly working on defining a roadmap of integration and validation.
Work carried out by beneficiaries (M13-M16)	The task has not started yet.
Work carried out by beneficiaries (M17-M24)	**MCI**: Establishing the initial lines of work on detailing the technology assets and recommendations. **ATOS**: Establishing the initial lines of work on detailing the technology assets and recommendations.

5.4.6 Meetings/calls in WP5

Date	Location	Reason
26 Feb 2020	Conference Call	GA meeting: definition of WP's work plan

5.5 Work Package 6: Dissemination and Exploitation

WP Leader: ORA

Contributors: All

5.5.1 Progress towards the objectives

Dissemination and Exploitation is a transversal work package that covers the entire implementation of the project and aims at creating awareness of the project and its results and at maximizing the impacts of the project towards the relevant stakeholders.

During Year 2, and contrary to Year 1, we have better balanced the work of this WP between on one hand dissemination/communication and on the other hand exploitation/business plan.

As shown in Section 4 of this report, on the first item (related to T6.1 on Dissemination and Communication), we have organized and have participated in several scientific and non-scientific manifestations. The nature of those events is very wide: conferences, workshops, summer schools, exhibitions, etc. Deliverable D6.3 better provides an in-depth study of what has been done on dissemination and communications since the beginning of the project, together with what is planned now.

On the second item (related to both T6.2 on Exploitation and T6.3 on Market Analysis and Business Plan), the objectives consists in using the PAPAYA results to create value for both industrial and non-industrial partners. As already explained in the Year 1 report, the work in T6.2 and T6.3 is done in close relation with the one in T1.3 on Innovation Management. The conclusion of the work done from now on this aspect is given in Deliverable D6.4 on Intermediate Business

Plan and Exploitation Report. This deliverable presents a macro environment analysis, summarizing the most important Political, Economical, Societal and Technological aspects that are shaping the current security landscape. It also gives some direct commercial competitors and focuses on actors on Privacy Enhancing Technologies (PETs). It then provides a first overview of the exploitation plan, explaining what is our view for a general consortium exploitation strategy, but also for a joint one, between partners, and finally for each member of the consortium individually. The business plan is finally described for each industrial partner, adopting the business model canvas.

5.5.2 Deviations

N/A

5.5.3 Task 6.1: Dissemination & Communication

Task Leader	ORA
Contributors	All
Overall task progress	The PAPAYA partners were involved in multiple and various dissemination and communication activities, creating awareness about the project.
Work carried out by beneficiaries (M13-M16)	**EURC**: EURECOM has participated to several different events related to PAPAYA. M. Önen chaired the IFIP summer school on Privacy and identity management. Together with MCI, ORA and IBM, a paper on PAPAYA primitives is submitted to this event. Also O. Ermis co-organized a workshop together with POSEIDON. M. Önen was also invited by Poseidon to Coimbra in July 2019. Finally, our poster on PAPAYA primitives won the best poster award in PUT 2019 which was held in conjunction with PoPets in July 2019. **IBM**: Contribution to IFIP summer school paper; Promotion of PP technologies being developed in PAPAYA across IBM research **KAU**: KAU participated to the dissemination activities and gave presentations. Co-organised PUT 2019 and the CBMS conference workshop. **MCI**: MCI participated to the dissemination activities. **ORA**: Different kinds of dissemination activities, especially related to Twitter and LinkedIn accounts, and website (in relation with Atos). **ATOS**: fine tuning and refining the website functionality. Updating the website's content.
Work carried out by beneficiaries (M17-M24)	**EURC**: EURC has contributed to several dissemination activities (keynotes, summer schools, etc.) **IBM**: Presenting PAPAYA technologies at Privacy&Security Seminar in Haifa **KAU**: KAU has been involved in writing 3 papers for disseminating project results (1 accepted and 2 submitted). Besides, KAU presented PAPAYA at a ENISA-ULD workshop on pseudonymity, and at a panel discussion organized by the Cyber Sec4Europe project and at the NECS winter school.

	MCI provided contributions on use cases for the publications released in the considered period. **ORA**: Dissemination activities related to Twitter account and web site. Creation of a proposal that will be submitted to the next Orange Research Show next December, based on Orange use cases

5.5.4 Task 6.2: Exploitation

Task Leader	ORA
Contributors	EURC, IBM, MCI, ATOS
Overall task progress	Submission of D6.4. Industrial partners have worked on the way to internally exploit PAPAYA's results.
Work carried out by beneficiaries (M13-M16)	EURC: EURC has being integrating PAPAYA finding to its lectures. IBM: Meetings with Israeli population and immigration authority to exploit PAPAYA technologies MCI: MCI contributed to the identification of exploitable assets and preliminary contributions to D6.4. ORA: The work on D6.4 related to exploitation has started. Review of existing work, recovery of work already done and proposal of a table of content for the deliverable. ATOS: Contributing to the corresponding deliverables, especially on the description of the Privacy Engine Exploitation
Work carried out by beneficiaries (M17-M24)	EURC: EURC has proposed several semester projects whose topics are PAPAYA related. IBM: Meetings with different bodies within/outside the IBM to exploit technologies being developed in PAPAYA MCI: In line with T1.3, MCI identified exploitable assets and their interactions (through the usage of the innovation questionnaires), which forms the needed basis to understand the possible exploitation plans (individual and of the consortium) to be presented as an outcome for this task. ORA: Interaction with the Flux Vision team at Orange Business Service to integrate PAPAYA's work on Bloom filters and trajectory clustering into their service. Interaction with different services inside Orange for the exploitation of the use cae related to statistics on mobile apps. ATOS: Contributing to the corresponding deliverables, especially on the description of the Privacy Engine Exploitation

5.5.5 Task 6.3: Market Analysis and Business Plan

Task Leader	MCI

Contributors	All
Overall task progress	The partners have been working on the market analysis and business plan, also with the support of the work conducted during T1.3.
Work carried out by beneficiaries (M13-M16)	EURC: EURC has contributed to the market analysis IBM: continue studying the market, understanding business needs and identifying competitive solutions. MCI: MCI contributed to the market analysis and the definition of its business plan. ORA: The work on D6.4 related to the business model has started. Recovery of work already done, based on questionnaires. ATOS: Contributing to the corresponding deliverables
Work carried out by beneficiaries (M17-M24)	IBM: Contribution to D6.4 MCI: in line with T1.3, MCI coordinated the analysis of existing market and products through the usage of the innovation questionnaires. ORA: Participation to the market analysis and business plan. ATOS: Contributing to the corresponding deliverables

5.5.6 Meetings/calls in WP6

Date	Location	Reason
May 29, 2019	Conference call	Innovation/Exploitation call
September 19, 2019	Conference call	WP6 meeting
September 30, 2019	Conference call	WP6 meeting
February 26, 2020	Conference call	WP6 meeting during the GA meeting
October 20, 2020	Conference call	WP6 meeting during the GA meeting
March 15, 2021	Conference call	PAPAYA Workshop with Business Units
April 13, 2021	Conference call	WP6 meeting during the GA meeting
June 22, 2021	Conference call	WP6 meeting
July 6, 2021	Conference call	WP6 meeting
July 20, 2021	Conference call	WP6 meeting

6 Deliverables, Milestones & Risk Management

6.1 Deliverables

Table 78 shows the status of all year 2 deliverables. As shown in this table, all deliverables were submitted on time. According to the Project Officer's and reviewer's feedback an additional document complementing D4.1 and describing the end-users of each PAPAYA component has been submitted.

Table 7 PAPAYA Year 2 deliverables

Del. No.	Deliverable Name	WP No.	Editor	Type	Diss. Level	Due Date	Actual Delivery Date	Status	Comments
D3.2	Risk Management Artefacts for Increased Transparency	WP3	KAU	R	PU	M15	M15	Delivered & Accepted	No further comments.
D4.1	Functional Design and Platform architecture	WP4	IBM	R	PU	M15	M15	Delivered & Accepted	An additional report describing the end-users of each component has been provided at M21
D6.3	Intermediate Dissemination and Communication report	WP6	ORA	R	CO	M18	M18	Submitted	No further comments
D6.4	Intermediate Business Plan and Exploitation Report	WP6	ORA	R	CO	M18	M18	Submitted	No further comments
D1.4	Second Project Progress Report	WP1	EURC	R	PU	M24	M24	Submitted	No further comments
D3.3	Complete Specification and Implementation of Privacy Preserving Data Analytics	WP3	ORA	R	PU	M24	M24	Submitted	No further comments
D3.4	Transparent Privacy preserving Data Analytics	WP3	KAU	R	PU	M24	M24	Submitted	No further comments

6.2 Milestones

Table 89 describes the status of the project with respect to the project's milestones corresponding to year 2, as defined in the DoA and the internal milestones as defined in deliverable D1.1.

Table 8 PAPAYA Year 2 milestones

MS No	Milestone title	Related WP(s) & Due Date	Means of achieved verification	Status	Comments
MS2	PAPAYA platform architecture description	WP4, M15	**MS2-1, M12** SotA analysis of selected platform technologies	Achieved	This analysis will be reported in D4.1
			MS2-2, M15 PAPAYA architecture, D4.1	Achieved	The architecture is described in D4.1.
MS3	PAPAYA analytics implementation	WP3, M24	**MS3-1, M6** SotA analysis v1	Achieved	SotA on cryptographic building blocks provided
			MS3-2, M12 SotA analysis v2, PAPAYA PETS v1, D3.1	Achieved	D3.1 delivered and includes SotA analysis and PAPAYA PETs
			MS3-3, M24 PAPAYA PETS v2, D3.3	Achieved	D3.3 provides the complete specification of PAPAYA PETs
MS4	PAPAYA transparency method description	WP3, M24	**MS4-1, M6** SotA on visualisation	Achieved	SotA analysis on visualisation tools is finalized
			MS4-2, M15 Identification of Risk management artefacts (D3.2)	Achieved	D3.2 describes the identified artefacts
			MS4-3, M24 Privacy preferences, Artefact visualisation(D3.4)	Achieved	D3.4 describes visualisation modules for privacy preferences and artefacts
MS5	Intermediate version of the PAPAYA platform	WP3, WP4, WP5, M30	**MS5-1, M24** Analysis of PAPAYA PETS and integration of one module at least	Achieved	The security analysis and performance evaluations of PAPAYA PETs are reported in D3.3. 3 modules (privacy preserving NN based on 2PC , privacy preserving collaborative training and privacy preserving NN classification based on hybrid approach) are integrated in the architecture. The Platform Dashboard is also integrated.
			MS5-2, M30 PAPAYA platform v1 (D4.2)	ongoing	This version of the platform will contain: (1) PP NN classification based on 2PC, PHE and hybrid approaches; (2) PP collaborative training of DNN; (3) IAM and Key Manager; (4) 1st version of Platform Dashboard including auditing; (5) 1st version of Data Subject tools including data disclosure view, annotated log view, first integrated versions of views for explaining

					privacy-preserving data analytics, and Privacy Engine. The rest of the services described in D4.2 will be integrated by M36

6.3 Risk Management

Table 10 overviews the identified risks and their status at year 2.

Table 9 PAPAYA status on risk management

Risk No	Risk Description & Initial level of Likelihood	Related WP(s)	Proposed mitigation measures (DoA)	Risk Status	Comments
RT1	Requirements are too ambitious and cannot be met. (*Low)*	**WP2, WP3, WP4, WP5**	The project will keep requirements in line with the objectives, and leaders of WP3 and WP4 will constantly review the requirements.	*Low*	D2.2 has defined a list of legal, HCI and platform requirements that are in line with the objectives. Both WP3 and WP4 members reviewed this list and defined acceptance criteria for each requirement.
RT2	Some use cases are discovered to be limited. *(Low).*	**WP2, WP5**	All partners will take part in the definition and the review of the use cases. Complementary adjustments can be made continuously during the project and reviewed at the WP5 start time. Interaction with operational team by industrial use case partners will additionally be done all along the project	*Low*	D2.1 defines a set of 5 general use cases illustrating the four usage scenarios defined in the DoA. These use cases cover different architecture settings and different machine learning algorithms. Additionally, the use of the PAPAYA components with its end-users is illustrated for each use case.
RT3	Failure to implement one or more primitives in a real setting *(Medium).*	**WP3, WP4, WP5**	WP3 partners will focus on most important requirements and innovative aspects and define a two-phase validation procedure in order to early detect any possible difficulties	*Low*	The complete specification and implementation of the the PAPAYA privacy preserving data analytics has been provided and described in D3.3
RT4	Delay in the development of the platform (*Low).*	**WP4**	The work by WP3 and WP4 will continuously be monitored which will allow identifying any possible delays and hence taking the necessary corrective measures such as focusing on key primitives that can be	*Mediu m*	At this stage of the project, there is no delay in the development of the platform. Nevertheless, the integration of individual WP3 modules will take more time than expected.

			validated by case studies.		
RT5	Time for development is underestimated (*Medium).*	**All WPs**	The project will focus on the core functionalities that can illustrate the key innovations of PAPAYA.	*Medium*	At this stage of the project there is no deviation with respect to the time for development. MCI will also join integration tasks.
RM1	Some potential conflicts regarding authorship or exploitation (*Low)*	**WP1**	The IPR strategy is defined in WP1 and provides a framework for managing authorship and results exploitation involving all partners. An early detection of such an issue will be done thanks to close and good contacts and frequent meetings.	*Low*	At this stage of the project, there are no conflicts among partners. The different innovation assets and their owners have already been defined and updated (see section 3).
RM2	Allocated resources are not sufficient (*Medium)*	**WP1**	Depending on shortage e.g. skills, expertise, etc. redistribution of the effort/costs can be proposed	*Medium*	There were some deviations reported in PPR1 and in this report but these were not major. (see section 8)
RI1	Project objectives lose relevance (*Low)*	**WP1, WP6**	T1.3 will produce an innovation strategy at the early stage to evaluate market trends. Industrial partners will bring their competences and will monitor and adapt the results in order to ensure the relevance of the solutions.	*Low*	Relevance of recognized assets (as an outcome to the project) has been also tracked with two different rounds of questionnaires (see Section 3), which monitored the adherence of the assets to the market
RI2	Results produced by PAPAYA are not well exploitable (*Low).*	**WP6**	T1.3 on innovation management will continuously monitor the market trends to influence WP action plans on time to redesign or incorporate new requirements. The presence of major industrials as well as partners that are key stakeholders allows PAPAYA to cover the complete value chain which in turn	*Low*	Exploitation of recognized assets, as well as their adherence to market expectations, has been evaluated while compiling the questionnaires mentioned in Section 3, at M12 and M24. The exploitation report has been submitted on time (M18) and each industrial partner has now a clear view on its own exploitation, in term of platform and/or use case As initially planned, we are now entering the second phase

			guarantees a variety of exploitation tracks.		for exploitation and business plan, which consists in refining the initial status given in D6.4.

Appendix 1 Technical note on End-users of PAPAYA Components (submitted on January 22nd 2020)

The goal of this technical note is to overview the architecture of the PAPAYA framework and highlight the end-users for each of the components. Additionally the document also clarifies which components are particularly used in each of the PAPAYA use cases together with the information on the involved end-users. We first provide a high-level overview of the architecture of the PAPAYA framework and present the main components and the actual stakeholders. We further identifiy the end-users for each component of the PAPAYA framework. Finally, we overview the PAPAYA use cases while highlighting the actual PAPAYA components and the end-users involved in each of them.

6.4 PAPAYA Framework

The PAPAYA framework (see Figure 1) is composed of two main groups of components: (1) the platform-side components that will be running on the (non-trusted, but semi honest) Kubernetes[4] cloud server; and (2) client side components, that will be running on trusted client environment. On a high-level, there are four main stakeholders in the PAPAYA framework:

1. ***Platform clients:*** stakeholders who wish to perform some analytics in a privacy preserving manner. ***Platform clients*** can be considered as Data Controllers or external queriers who are allowed to request some analytics results while not being the actual owners of the data.
2. ***Platform administrators:*** responsible for platform administration purposes such as resource allocation or monitoring.
3. ***Service providers***: the author of the services available on the platform.
4. ***Data Subjects: end-users (e.g. application user)*** of the ***Platform clients***.

[4] https://kubernetes.io/

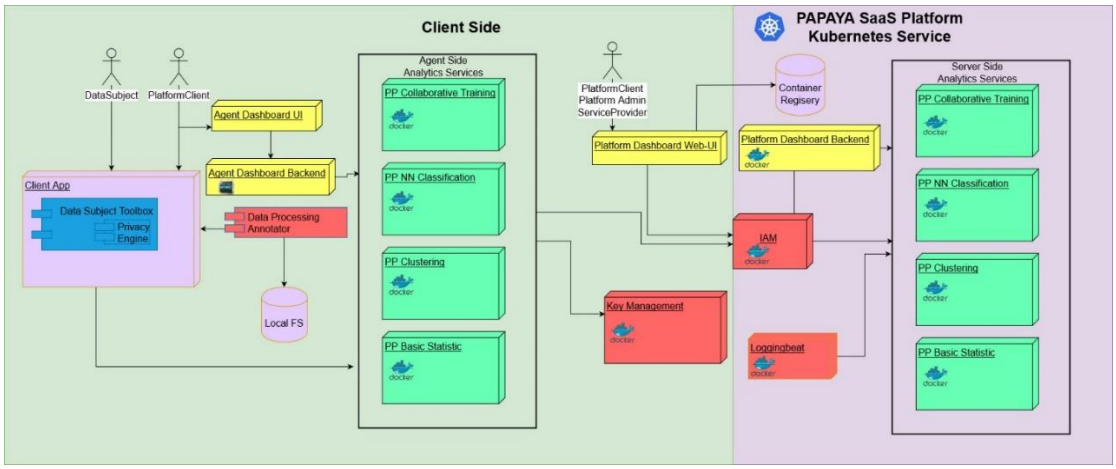

Figure 13 PAPAYA Framework architecture

From the functional perspective, the PAPAYA framework components can be regrouped into the following categories (more details about each category can be found in deliverables D4.1 and D3.1):

- **The privacy-preserving analytics services** (colored with green in Figure 1) which will allow platform clients to perform analytics of interest, in a privacy-preserving manner. In the first version of PAPAYA we will support the following analytics:
  1. Privacy-preserving NN classification. We will provide four services for applying neural network for the purpose of classification in a privacy-preserving manner: (1) 2PC-based; (2) PHE-based; (3) FHE-based; and (4) Hybrid approach. Each one could be preferable than others in different settings, mainly depending on NN architecture
  2. Privacy-preserving collaborative training of NN. The service allows multiple participants to perform a ML training collaboratively, while preserving the privacy of the training data.
  3. Privacy-preserving trajectory clustering. The service provides means to cluster trajectories in a privacy preserving manner.
  4. Privacy-preserving basic statistics. The service provides means for privacy-preserving computation of statistics using functional encryption and privacy-preserving counting using Bloom Filters.

The users of these services are ***platform clients*** who can either be Data Controllers or external queriers (in the case for privacy preserving trajectory clustering who are authorized by Data Controllers to request some analytics results***.*** Each service is divided into two parts:

1. Server – responsible for performing analytics of interest on encrypted data and will run on a PAPAYA's Kubernetes cluster.
2. Agent – responsible for communication with the appropriate server-side component and responsible for managing cryptographic operations for the client. The agent will

be downloaded from the Container Registry (CR) as a Docker image and deployed on a client side. Deployment and execution will be under the responsibility of the platform client.

- **The platform security and transparency services** (colored with red in Figure 1) which will provide platform authorization, authentication (Identity and Access Management - IAM), auditing and cryptographic Key Manager (if needed).

- **The PAPAYA dashboards** (colored with yellow in Figure 1):

  1. **Platform dashboard** will allow: (1) **service providers** to deploy privacy-preserving services; (2) **platform clients** to choose/run privacy preserving services, and review operational and auditing logs; and (3) **platform administrators** to configure and manage the platform.
  2. **Agent dashboard** will allow **platform clients** to visualize the configuration of the agent running on the client side and review operational and auditing logs.

- **Data Subject Toolbox** (colored with blue in Figure 1) consists of a number of mostly independent tools (DS Tool 1: Explaining Privacy-preserving Analytic, DS Tool 2: Data Disclosure Visualization, DS Tool 3: Annotated Log View and DS Tool 4: Privacy Engine), which provide versatile tools for data protection by design by platform clients (acting as data controllers) towards data subjects whose personal data is processed in their services.

6.5 End-users of PAPAYA Components

Table 13 overviews each PAPAYA component and identifies the corresponding end-user(s).

Table 10 End-users of each PAPAYA Framework component

Component	Description	End-user
PP-NN classification	Neural Network classification service. There are four components who deliver this service. They mainly differ with respect to the underlying cryptographic technique	Platform clients (Data Controllers)
PP-Collaborative training	Collaboratively training a Neural Network model.	Platform clients (Data Controllers)
PP-trajectory clustering	Clustering service for trajectory information.	Platform clients (Data controllers, external Queriers)

PP-Basic statistics	Basic statistics computation service. These include set union and set intersection operations	Platform clients (Data controllers, external queriers)
PP Counting	Basic occurrence counting service.	Platform clients (Data Controllers, External Queriers), Data Subjects
IAM	Authentication and Authorization service for the Platform.	Platform administrator (configuration of IAM), platform client (user of IAM).
Auditing	Auditing/ logging service for transparency purposes	Platform clients, Platform administrators
Key Manager	Key Management service	Platform client (Data Controller)
Platform Dashboard	Dashboard for Platform administration	Platform administrators, Platform clients, service providers
Agent Dashboard	Dashboard for service providers	Platform clients
DS Tool 1	This tool explains PAPAYA's Privacy-preserving Analytics services with the potential risks	Data Subjects, Platform Client (Data Controller)
DS Tool 2	Data Disclosure Visualization Tool which visualizes which data is disclosed to which party	Data Subjects, Platform Client (Data Controller)
DS Tool 3	Annotated Log tool which explains the actual operation that has take place on relevant personal data	Data Subjects, Platform Client (Data Controller)
DS Tool 4	Privacy Engine	Data Subjects, Platform Client (Data Controller)

6.6 Users of PAPAYA Use Cases

In this section, we overview the five PAPAYA use cases and highlight the components and the end-users involved in each use case.

Table 11 End-users involved in each PAPAYA use case

Use Case	Components	End-users
Privacy preserving arrhythmia detection (UC1)	PP components: - PP NN classification DS tools: - DS Tool 1	See figure 16
Privacy-preserving stress management (UC2)	PP components: - PP collaborative training DS tools: - DS Tool 1 - DS Tool 2 - DS Tool 4	See figure 17
Mobility analytics (UC3)	PP components: -PP-trajectory clustering, PP-Basic statistics, PP-counting	See figure 18
Mobile usage analytics (UC4)	PP components: - PP counting DS tools: - DS Tool 1 - DS Tool 2 - DS Tool 3 - DS Tool 4	See figure 19
Threat detection (UC5)	PP components: - PP NN classification	See figure 20

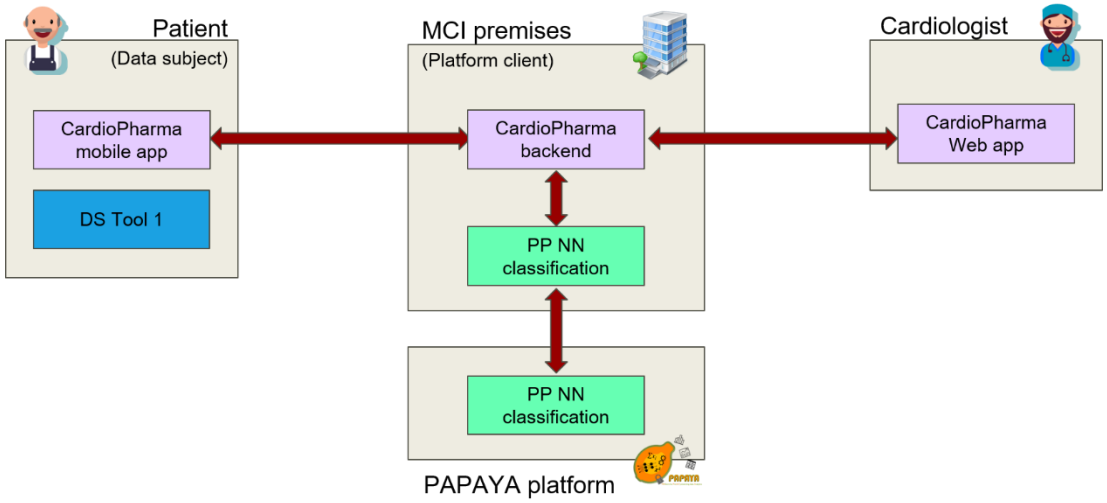

Figure 14 UC1: Privacy preserving arrhythmia detection

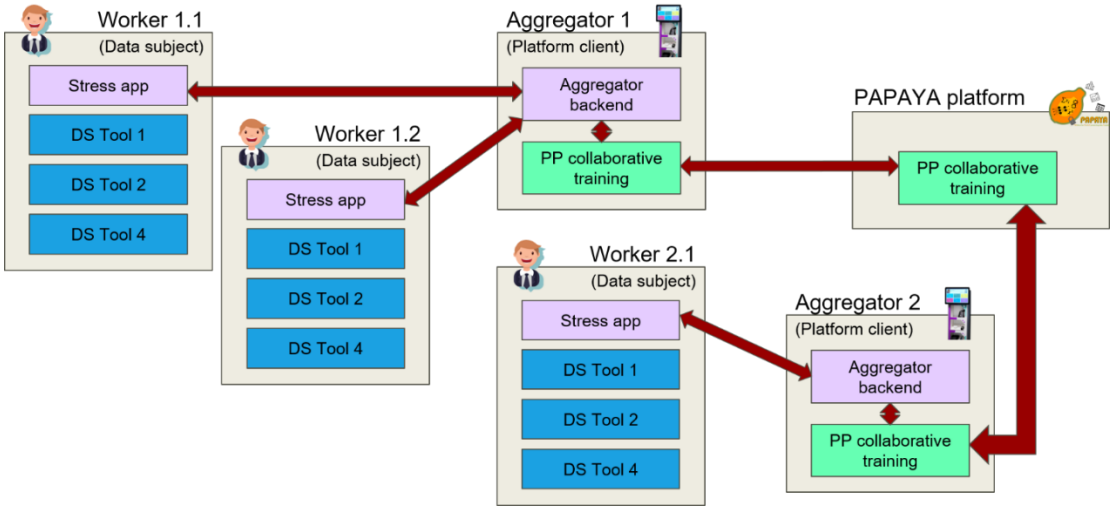

Figure 15 UC2: Privacy preserving stress management

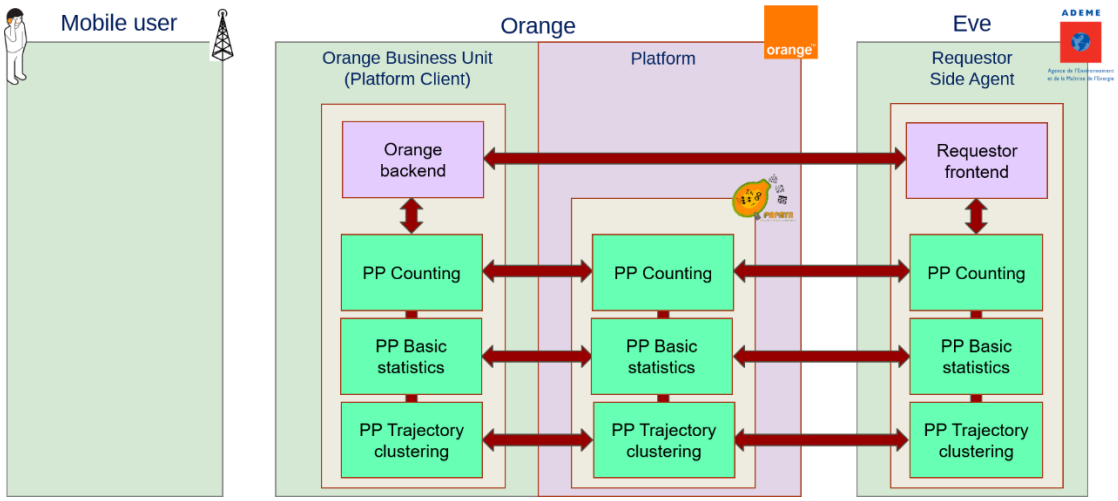

Figure 16 UC3: Mobility analytics

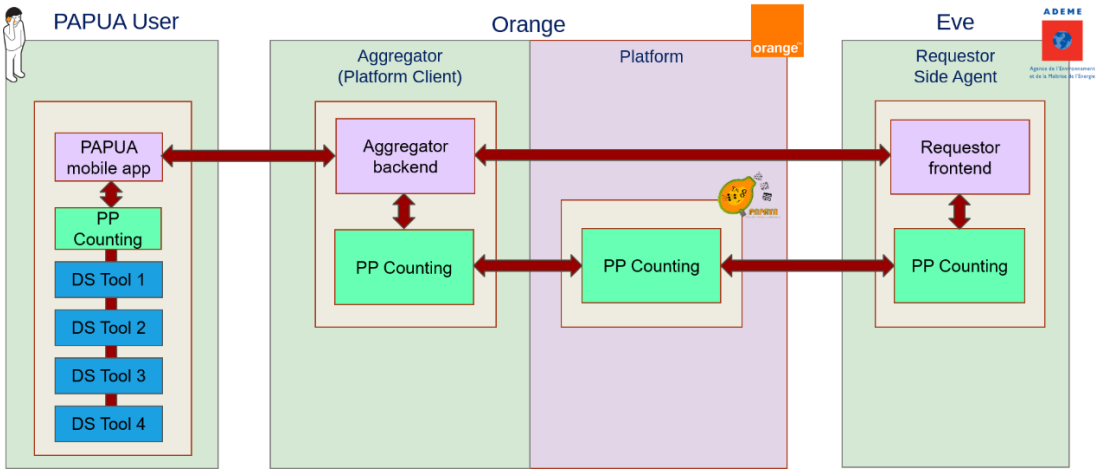

Figure 17 Mobile usage analytics

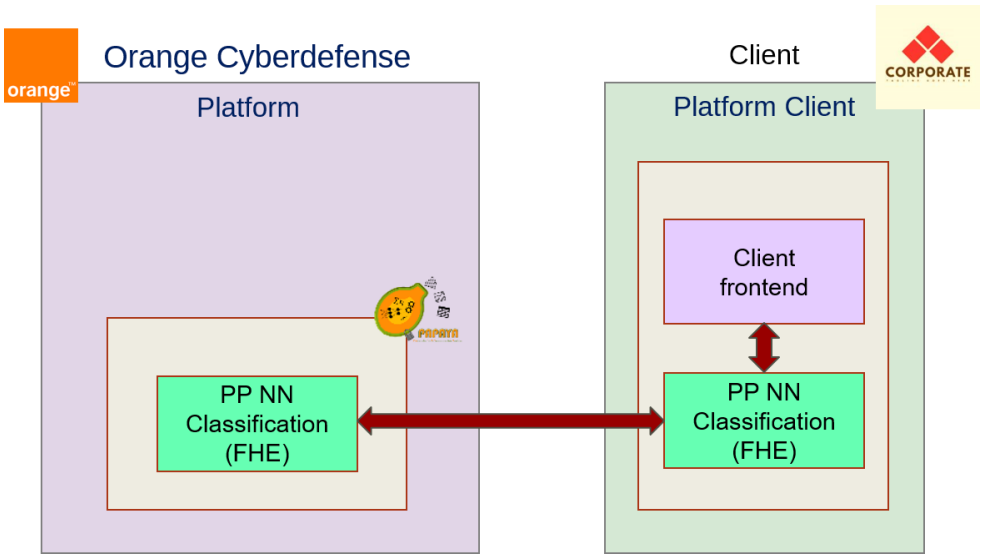

Figure 18 UC5: Threat detection

Appendix 2

Due to the starting of the Covid19 pandemia in Northern Italy, the PAPAYA General Assembly meeting which was scheduled on February 25th and 26th was cancelled. The table below summarizes the relevant costs and the cancellation fees per partner. These fees will be declared along with the financial statement during the next periodic report and all corresponding invoices will also be provided. Partners request EC's approval for these costs.

Trento GA Meeting cancellation fees due to Covid19 pandemia					
Partner	**Cost type**	**Initial Cost**	**Cancellation fee**	**Refund received**	**Difference to be claimed**
EURC	**Nothing to claim**	**N/A**	**N/A**	**N/A**	**N/A**
IBM	**Flight cost**				
	Boris Rozenberg,	805.10 $	51 $	341.26 $	514.84 $
	Ron Shmelkin,	805.10 $	51 $	341.26 $	514.84 $
	Allon Adir	465.16 $	25.50 $	354.36 $	136.30 $
	Total	**2075.36 $**	**127.50 $**	**1036.88 $**	**1165.98 $**
KAU	**Flight & Hotel cost**				
	Tobias Pulls (flight)	3372 SEK		596 SEK	2776 SEK
	Tobias Pulls (train)	1096 SEK		1096 SEK	0 SEK
	Tobias Pulls (train)	175 SEK		175 SEK	0 SEK
	Tobias Pulls (hotel)	1428 SEK		0 SEK	1428 SEK
	Tobias Pulls (hotel	753 SEK		753 SEK	0 SEK
	Total	**6824 SEK**		**2620 SEK**	**4204 SEK**
MCI	**Nothing to claim**	**N/A**	**N/A**	**N/A**	**N/A**
ORA	**Nothing to claim**	**N/A**	**N/A**	**N/A**	**N/A**
ATOS	**Flight cost**				
	Ángel Palomares	517.02 **€**	0 **€**	0 **€**	**517.02 €**
	Total	**517.02 €**	0 **€**	0 **€**	**517.02 €**