Towards an Open, Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem

D1.6 Ethics Issues Management Plan

Project Number	**730929**
Start Date	**01/01/2017**
Duration	**36 months**
Topic	**ICT-06-2016 - Cloud Computing**

Work Package	**WP1, Project Management**
Due Date:	*M12*
Submission Date:	*22/12/2017*
Version:	*0.6*
Status	*Final*
Author(s):	*Lara López (ATOS)*
Reviewer(s)	*Blanca Jordan (ATOS)* *Xavi Masip (UPC)*

Keywords
Ethics, privacy, security, management

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group specified by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	**X**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730929. Any dissemination of results here presented reflects only the consortium view. The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	19/09/2017	Initial ToC and assignments	Lara López (ATOS)
0.2	09/11/2017	UC inputs	Antonio Salis (ENG), Matjia Cankar (XLAB), Francisco Hernandez (WOS)
0.3	04/12/2017	Sections 2, 3, 4 and 5. Development of Terms & Conditions	Lara López (ATOS)
0.4	14/12/2017	First integrated version ready for internal review	Lara López (ATOS)
0.4	15/12/2017	Internal review	Xavier Masip (ATOS)
0.5	19/12/2017	Ethics Expert assessment	Blanca Jordán (ATOS)
0.6	22/12/2017	Final version and quality check	Lara López (ATOS)

Table of Contents

List of figures

List of tables

Executive Summary

The present document analyses all ethics consideration for the three project use cases: Emergency Situation Management in Smart City, Enriched Navigation Service and Smart Fog-Hub Service. At the beginning of the project all of them were leading with personal data. However, after some technical and legal considerations the scope of Use Case 1: Emergency Situation Management in Smart City has changed and now no personal data is managed.

Special considerations from the new GDPR, which will come into force in May 2018, has been also taken into account to provide the most accurate assessment as possible.

1. Introduction

1.1 Purpose

The objective of this deliverable is to identify the ethics principles that the project must accomplish as well as the new regulatory framework coming into force in May 2018. Specific issues per use case have been also analysed.

The document is structure into 4 main sections:

Section 2, identifies all rules for the project.

Section 3, defines the governance rules for the project and the specific role of the Ethics Expert.

Section 4, lists the regulations to be taken into consideration within the project lifetime.

Section 5, presents the specific ethic issues per use case.

1.2 Glossary of Acronyms

Acronym	Definition
UC	Use Case

Table 1. Acronyms

2. Ethical principles

This section contains the basic rules to be followed by the mF2C project according to OECD recommendations [1]:

1. The project will implement mechanisms to ensure the protection of data privacy. Openness will be considered only under the correspondent legal and ethical constraints.
2. The project will develop an informed consent to be signed by the subject of research prior to collect, process or share it.
3. The project will ensure transparency within the purpose and kind of data collected.
4. The project will develop a list of risks per each UC before collecting data in order to identify potential negative consequences in advance, and thus develop the correspondent mitigation plans.
5. The project must ensure the quality of the data shared.
6. The project will fairly distribute responsibilities between the data owner and the data manager.
7. The project must be assessed by an Ethics Expert and implement her advices.
8. Data holders' roles must be clearly defined per UC within the project.
9. Data will be anonymised. If this is not possible, data controllers and processors must fulfil the GDPR as a whole, based on the Accountability principle.
10. Data anonymization techniques must be correctly applied and guarantee irreversibility or non-re-identification.
11. Proactive actions will be adopted to protect information and offer additional guarantees to be assessed by the Ethics Expert.
12. In case it is needed, each organization will demonstrate that is capable by its own of implementing measures to fulfil the regulation in their ordinary business.
13. All partners from countries where data protection officers are not compulsory must check if there is the need for registering into the National Data Protection Authority register.

3. Research Governance

Research Governance is defined as "*the broad range of regulations, principles and standards of good practice that exists to achieve, and continuously improve, research quality [nationally and internationally]"* [2].

The main aim of this governance model is to ensure the protection of participants, data and research results, dealing with the applicable legislation, listed in the following section.

In order to be compliant with this model, mF2C has appointed an Ethics Expert, who is also a reviewer of this document, to ensure that the main ethics principles are covered within the project. The Ethics Expert is external to the project in order to ensure its independency from the project management, having and advisory status.

The main responsibilities of the Ethics Expert are:

- Assess the compliance with the data protection requirements/regulation.
- Assess the informed consent to be provided within each UC.
- Review the protocols implemented by the project.
- Conduct an ethical review of the experiments.
- Review and approve/reject/suggest modifications regarding the ethics procedure.

4. Legal frameworks

In D1.1 Project Plan, European legislative framework was analysed. Directives and regulations identified there are reproduced here:

- **Regulation 2016/679** [3] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- **Directive 95/46/EC** [4] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- **Directive 2002/58/EC** [5] of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.
- **Directive 2016/680** [6] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection of prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

5. Specific issues

Additional considerations for each UC are specified in the following subsections.

5.1 Special considerations for Use Case 1

The envisage UC1 for mF2C was based on the exploitation of distributed traffic control technologies (Bitcarrier) and the company's mobility platform that ingests and analyses the input data, providing Operational Intelligence capabilities to the end users. This concept would take as a reference the real deployment in Bogota (Colombia), where a non-EU legislation applies. There, the installation of these technologies which potentially acquires personal data, are subject to the National Legislation (Colombian law 1581/2012) [7], which formally is quite similar to the current Spanish legislation (Ley Orgánica 15/1999) without any huge difference in most of the main provisions.

Since the Bogota's mobility platform has been developed in the frame of a public tender in Colombia, Worldsensing has implemented the specific technologies taking into account the abovementioned legislation. Actually, the MAC addresses related to the Wi-Fi and Bluetooth devices owned by citizens (i.e. smart devices) are anonymized, and the system works without the identification of people running on the street. The first step is done in the Bitcarrier layer (traffic flow monitoring), and it has also been applied to the devices installed in some motorways in Barcelona (Spain) and other locations in Europe without contradiction with the applicable EU legislation.

In this context, it should be pointed out that this action goes beyond the Colombian requirements since the MAC addresses are considered semi-private data, which are not subject to Data Protection if they are used for public monitoring purposes, like in this case. The end users are the public authorities from Bogota, who are the ultimate responsible for assuming the risk and assess the compliance with the Colombian legislation.

The technical problems of adapting this use case to the mF2C scenario and the potential issues that Bitcarrier could present once the new GDPR comes into force in May 2018 have been decisive to rule out the traffic UC for the project. Now, Worldsensing in agreement with the rest of the consortium proposes a more conservative approach in which the industrial IoT acquisition system monitoring structural information from buildings, such as tilting and vibration, has been selected to implement a mF2C UC. Here, no personal data is used.

5.2 Privacy

The Use Case 3 is based in a public crowded environment (airport area) with a relevant number of objects that are related to passengers and partners, or people that work in this environment.

The defined service, provided through an Android app, is oriented to track and engage all people in the field offering information, suggestions on the best way to use available services, e.g. suggest the moment for shorter waiting times in Security Control to departing people, to move close to the gate or notify the final call, or recommend relevant proposals and offerings in shops close to the user (proximity marketing). All these suggestions can be refined according to behaviour and choices done by passengers.

Since all referenced objects are owned by people, some personal identifiable information is managed (only if the user decides to sign up).

The proposed service will be provided by means of an Android app, which has to be downloaded and installed from Google Play. The downloaded file will include both mF2C agent and the specific application.

The expected treatments are basically the following:

- Object tracking with wifi positioning; only in case of app installation the user registration step will be done, thus relating user identity and position tracking, otherwise object tracking will be done anonymously;
- Service provision, navigating in the app, receiving advices and promotions in shops nearby, information on departing flights, etc.
- Forecasts and recommendation, based on people behaviour, movements or recurrent paths.

5.3 Consent

At the moment of installation of the App an informative page will be presented to the user, highlighting the specific personal information treatments that will be performed, so clicking on the "Accept" button the user will accept the established **Terms & Conditions**.

The basic flow will be as follows:

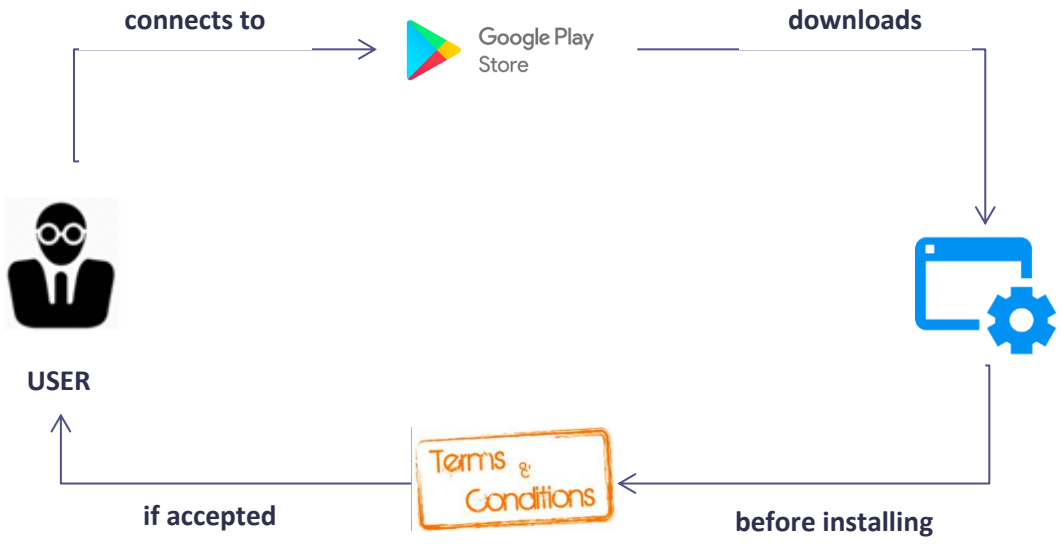

Figure 1 Smart Fog-Hub workflow

Annex 1 contains a summary of all the information that must be provided to the final end user in a written form. However, the text for the online form must be adapted in order to ensure that the user reads and understand the content.

A short paragraph explaining what kind of information will be collected and for what purposes will be presented to the user, together with additional extended documentation to be consulted at any time.

5.4 Anonymity and de-identification

Provided that user personal data are managed only in case of signup, otherwise the object will be tracked anonymously. All information collected in the smartphones or personal devices will be securely stored and transferred. In case of use of Machine Learning algorithms to determine preferences, recommendations, forecasts on behaviour, the collected data will be anonymized before using it. No kind of user categorization or profiling will be performed.

5.5 Commodification of data

In this context, the term 'commodification' refers to the conversion of raw data into information expecting revenue from it.

Based on this assumption, no commodification of collected or managed data is expected.

5.6 Data sharing and security

Data sharing is not supported.

5.7 Public engagement

Public engagement is expected, restricted to the scope of the airport under study in UC3.

6. Conclusions (and Next Steps)

The information contained here will be updated before the project end in order to cover any potential update in the current legislative framework or change in the use case definition.

It is not planned within the project a variation in the nature of the collected data or even of its origin. However, in case there is no enough volume of data the causes will be deeply analysed. If finally, it is due to the acceptance of the Terms & Conditions, the text will be revised and updated to make it more legible for non-experts users.

Annex 1: Terms & Conditions template

Written consent documentation includes two differentiated parts: an Information Sheet and a Consent Form to be signed by the participant. mF2C has developed a generic Information Sheet that can be applied to the different project use cases with only minor adaptations, if needed, plus an unique Consent Form for the three of them.

Templates provided in this document are on a printable style, but they will be adapted to an electronic style, as expected in Section 5.3 for ensuring that the user can understand correctly what kind of personal data will be used and for what.

Informed Consent Form for *passengers in the airport/yatch patrons* **who we are inviting to participated in the research project "Towards and Open Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem (mF2C)" selected use case.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730929

The Informed Consent Form has two parts:

- Information Sheet (to share information about the study with you)
- Certificate of Consent (for signatures if you choose to participate)

You will be given a copy of the full Informed Consent Form

Part I: Information Sheet

Introduction

mF2C project aims to…

Each UC will provide the corresponding explanation according to their needs. This template will be updated with it prior to be released.

Purpose of the research

Geographical tracking of individuals is an important subject due to security reasons. However, within this project this information will be used to determine mobility patterns in order to improve individual quality of experience in certain locations.

Type of Research Intervention

This research will not involve your active participation as the information is collected directly from your device.

Participant Selection

You have been invited to take part of this research as a user of the underpinned applications. Your contribution will help us to improve our understanding and knowledge of user movements.

Voluntary Participation

Your participation in this research is entirely voluntary. It is your choice whether to participate or not. If you choose not to participate all the services you usually receive will continue and nothing will change.

Procedures

For this research you are invited to share your location using your mobile device. It will not be shared under the project neither with other third parties during the research period. No personal information such as beliefs, practices or stories will be collected.

Duration

The duration of the research is of 36 months and collected information will not be stored after that period.

Risks

The project is taking into account any security and safety consideration of data management regulation and will act according to European legislation.

Benefits

There is no direct benefit from the participation in the research apart from the improvement in the quality of experience.

Reimbursements

You will not receive any incentive for being part of the research case.

Confidentiality

Personal information will not be shared outside of this project. However, based on the anonymization of this data you can receive some suggestion for improving your experience.

Sharing the Results

The knowledge gained with this research will be shared but will not be made available for the public. Each participant will receive some suggestions based only on its data.

Right to Refuse or Withdraw

Participating in this research is not mandatory and, according to the current legislation, you can stop your participation at any time.

Who to Contact

For accessing/modifying/stopping participation you can contact the support organization:

Data to be provided by each use case owner

Part II: Certificate of Consent

I have read the foregoing information, or it has been read to me. I consent voluntarily to be a participant in this study.

References

[1] OECD, “Research Ethics and New Forms of Data for Social and Economic Research,” [Online]. Available: http://www.oecd-ilibrary.org/science-and-technology/research-ethics-and-new-forms-of-data-for-social-and-economic-research_5jln7vnpxs32-en.

[2] R. G. definition. [Online]. Available: http://www.imperial.ac.uk/joint-research-compliance-office.

[3] R. 2016/679. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[4] D. 95/46/EC. [Online]. Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046.

[5] D. 2002/58/EC. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.

[6] D. 2016/680. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC.

[7] C. l. 1581/2012. [Online]. Available: http://www.sic.gov.co/proteccion-de-datos-personales.