MAZI

ICT - Information and Communication Technologies

Project Acronym:	**MAZI**
Project Full Title:	**A DIY networking toolkit for location-based collective awareness**
Grant Agreement:	**687983**
Project Duration:	**36 months (Jan. 2016 - Dec. 2018)**

Ethics Requirements - Humans and Protection of personal data

Deliverable Status:	**Final**
File Name:	**MAZI_Requirements_POPD.pdf**
Due Date:	**30 June 2016 (M6)**
Submission Date:	**31 August 2016 (M8)**
Dissemination Level:	**Public**
Task Leader:	**Thanasis Korakis (UTH)**
Author:	**Harris Niavis (UTH),**
	Stavroula Maglavera (UTH)
	Panayiotis Antoniadis (NH),
	Ingi Helgason (NU)
	Andreas Unteidig (UdK)
	Mark Gaved (OU)
	James Stevens (SPC)

Consisting of:

Organisation Name	Short Name	Country
University of Thessaly	UTH	Greece
NETHOOD	NH	Switzerland
Edinburg Napier University	NU	United Kingdom
Universitat der Kunste Berlin	UdK	Germany
The Open University	OU	United Kingdom
Slacktivist Limited	SPC	United Kingdom
INURA Zurich Institute	INURA	Switzerland
Common Grounds	CG	Germany
UnMonastery	UM	United Kingdom

History

Version	Author	Date	Status
1.1	Stavroula Maglavera	15//6/2016	Draft
1.2	Ingi Helganson	16/8/2016	Draft
1.3	Stavroula Maglabera	19/8/2016	Draft
1.4	Mark Gaved	22/8/2016	Draft
1.5	Ingi Helganson	23/8/2016	Draft
2.1	Stavroula Maglavera	30/8/2016	Draft
FD	Stavroula Maglavera	5/9/2016	Final Draft
FF	Stavroula Maglavera	9/9/2016	Final

Executive summary - Introduction

The current deliverable aims to identify ethical issues and the protection of personal data that may arise within the implementation and deployment of MAZI.

MAZI collects, uses and involves only marginally personal data, while in most cases the data produced by the project refer to technical measures or experiments not involving human beings. Nonetheless, MAZI seeks the adoption of proper security and confidentiality standards for the data collected.

In addition, from the specific nature of MAZI and from its being part of CAPS initiative, it derives a particular emphasis on the involvement of citizens, stakeholders, user communities, research agencies, etc. All these considerations require the adoption of existing standards and regulations for the scientific dissemination of information, as set out in the Grant Agreement. In order to avoid problems and misunderstandings and to streamline the whole process of data collection and of dissemination of results, the current deliverable defines the data protection requirements and guidelines on how to treat personal data.

Table of Contents

1. Privacy issues

1.1 Ethical considerations

MAZI fully respects the rights of all citizens as described in the Charter of Fundamental Rights of the European Union and is committed to ethical and responsible research practice.

This document provides guidance to MAZI partners on data management, together with a checklist of questions for all partners to use to guide their own ethics self-assessment processes. The self-assessment process will help partners to identify and follow appropriate good practice guidelines as required. This document will be reviewed and updated during the lifetime of the project.

MAZI is subject to two types of data collection, online social interactions, interviews, workshops, questionnaires, recordings, surveys, etc, which are in general subject to the ethical issue of "Human Data Collection". In the following we refer to "Personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

1.2 Personal data produced by MAZI

MAZI does not intend to use or store any personal data collected from research participants before the start of the project.

MAZI research may involve participants in situations where collection of personal data is appropriate. However, it is expected that this data will not be of a highly sensitive nature. Efforts will be made by all partners to carefully consider the involvement of participants and the collection of personal data. Involvement of participants will at all times be voluntary.

At the time of writing it is expected that the project will produce the following types of data that may include personal information relating to individuals:

- Case study data from interviews, workshops, questionnaires, potentially including audio recordings, photos, videos etc.
- Case Study data from surveys, social media data and observational analysis.
- Platform usage data

Study in MAZI is considered any activity that contributes directly to research, and involves gathering data for research purposes (for example it might lead to published results). It is up to the researcher/partner managing the activity to decide if the work they are doing is a study or is some other activity. For example, a public meeting or conference would not be a study if it only for dissemination purposes. However there may still be ethical issues around (for example) taking photographs and putting these on a public website. It may be enough to tell everyone verbally that photos will be taken and that they can "opt out" if they choose.

1.3 Procedural method

The methodologies involve several well-defined steps, such as the selection of target persons, workshops including target persons, and evaluations. This means in detail that:

1. All volunteers that are included in studies will be clearly and fully informed, so that they are able to give meaningful consent to participate. This information will include explanation of; the purpose of the research, and procedures for handling, protection and storage of their data. Volunteers will be made aware of both the potential benefits and any identified risks of participation in the project.
2. Consent must be given freely, and evidence of consent recorded. It will be made clear to volunteers that they can refuse to participate at any time with no consequences, and their personal data will be deleted as requested.
3. Information and contact details will be given to volunteers so that they can get in touch with the project at any time after the study.
4. Informed consent forms will be written in the preferred language of the participants, and will be written in manner that is as clear and straightforward as possible.
5. Data management will comply with respective national data protection acts. Data will be anonymised, as privacy can be under threat if data is traced back to individuals. Stored data will not include the names or addresses of participants, and identities of individuals will be known only by the research partners directly involved.
6. Raw data such as interview text and audio files will only be shared within the consortium partners after signing the confidentiality agreement. (see appendix)
7. Information about participants will be edited for full anonymity before being processed, for example in project reports or scientific publications.

1.4 Data storage

Collected data will be stored on password-protected formats at the partner institution responsible for data collection and analysis. The data will be used only within the project and will not be made accessible for any third party.

After the end of the project, it will only be kept for enough time to allow for final publications, (expected to be around 2 years) unless required by relevant national legislation.

1.5 Self-assessment process

Any research activity undertaken within the MAZI project that entails the collection, storage, or handling of personal data will undergo a self-assessment check carried out by the relevant partner(s). This follows the principle of responsible and informed research practice, supported by continuous reflective questioning by all partners involved in the research process.

The main issues addressed by the self-assessment are; protection of identity and privacy, obtaining informed consent, and communicating benefits and risks to participants.

The MAZI self-assessment process entails considering the following questions, and keeping a record of the responses and justifications for the chosen approach:

1. What personal data will be gathered for the activity? How much is essential, and how can it be kept to the minimum necessary for effective research?

2. Will collected data be publicly available in any form? Should it be anonymised?
3. Is it necessary to obtain informed consent from participants for the collection of data, and if so, how will this collection be handled?
4. Could any of the participants in the study be described as "vulnerable", or potentially lacking the capacity to give valid consent, for example due to young age? If so, what ethical consideration is needed?
5. How will the records of informed consent be stored and kept confidential? Does this comply with relevant National Data Protection authorities?
6. Are any organisational, legal or ethical authorisations or approvals required for this activity? Are there any other good practice guidelines that will be followed, for example from the university or research institution?
7. Are there any other factors or potential risks concerning this activity that are relevant to the collection, storage and handling or personal data? How will they be handled?
8. Are there any potential negative or positive, intended or unintended consequences of the planned research that have not been addressed in the previous questions?

1.6 The European Framework for privacy protection

Under the European Union (EU) law, personal data is defined as "any information relating to an identified or identifiable natural person". The collection, use and disclosure of personal data at a European level are regulated in particular by the following directives:

- Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation) will be strictly followed by the project security model.
- Directive 95/46/EC on protection of personal data (Data Protection Directive)
- Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)
- Directive 2009/136/EC (Cookie Directive)

Directives generally do not directly apply in the EU and associated non-EU countries and need to be nationally implemented by each country through laws and regulations. As countries have some freedom in the implementation of directives, stricter requirements than those prescribed by the directives may apply in certain EU countries. Furthermore, the national data protection legislation is, in many respects, complemented or overlapped by sector specific legislation that also needs to be considered. Therefore, in order to get a clear and comprehensive picture of the data protection requirements, it is essential to check the national frameworks, national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations.

Specifically:

- ***Regulation (EU) 2016/679 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***

The Directive regulates the processing of personal data regardless of whether such processing is automated or not. The principle is that personal data should not be processed at all, except when certain conditions are met.

- Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."
- defines criteria for making personal data processing legitimate:
    - the data subject has given his/her consent

- processing is necessary for the performance of or the entering into a contract the data subject is party
- processing is necessary for compliance with a legal obligation the controller is subject
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed,

- ***Directive 2002/58/EC (Directive on privacy and electronic communications, also known as e-Privacy Directive)***

e-Privacy Directive concerns the processing of personal data and the protection of privacy in the electronic communications sector and deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies.

- *Article 5 Confidentiality of the communications*
  - Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15. This paragraph shall not prevent technical storage, which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
  - Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
  - Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

- ***Directive 2009/136/EC (Cookie Directive)***

This Directive amended Directive 2002/58/EC, requiring end user consent to the storing of cookies on their computer. Cookies are hidden information exchanged between an Internet user and a web server stored in a file on the user's hard disc. They can be used to monitor Internet activities of the user. The Directive states that the measures referred to in paragraph 1 Article 4 of the Directive 2002/58/EC shall at least:

- ensure that personal data can be accessed only by authorized personnel for legally

authorized purposes,

- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data.

2. General principles

2.1 Data security

Data should be secure from viruses, hacker attacks, forgery etc. Security means protection of information and information systems by ensuring confidentiality, availability, integrity, authentication, and non-repudiation.

- ***Confidentiality:*** Information is not made available or disclosed to unauthorized individuals and entities.
- ***Availability:*** Data/information have to be available, only authorized persons can remove it, in accordance to law
- ***Integrity:*** only authorized persons can modify the data/information, in accordance to law
- ***Authentication*** must be preserved (data/information must be authentic)
- ***Non-repudiation*** – participants will not be able to successfully challenge the authorship of the data provided

The privacy protection and operational model of MAZI follows three pillars:

- ***Data anonymity*** will be guaranteed whenever possible. The only exemption to anonymity can be in some cases for the researcher directly interacting with the participants in surveys. When data must be presented in non-aggregate ways for research purposes, the data will be anonymized. Furthermore, provisions will be taken to avoid the possibility of information linkage.
- The ***informed consent policy*** requires that each participant will provide his/her informed consent prior to the start of any activity involving him/her. ANNEX 1 includes a working template of the likely informed consent form that will be completed by participants in surveys and interviews. Public distribution of elements of information that can reveal the identity of the users (e.g., videos or pictures) for scientific dissemination purposes will be explicitly authorized by the participant as part of this process.
- To achieve a limited ***circulation of the information***, the database containing in anonymous form the data collected from the users (e.g., the results of questionnaires and of laboratory experiments) will be distributed to the partners, if needed at all, through protected and encrypted Internet connections; the raw data will only be shared if it is required for the development. The researchers will never pass on or publish the data without first protecting participants' identities. No irrelevant information will be collected; at all times, the gathering of private information will follow the principle of proportionality by which only the information strictly required to achieve the project objectives will be collected. In all cases, the right of data cancellation will allow all users to request the removal of their data from the project repository at any time.

3. Security requirements

In order to accomplish the creation of a security framework it is essential to focus on the issues of access and identity authentication, authorization and auditing (AAA). Therefore, our main objective is to develop a base security system that standardizes the processes of Authentication, Authorisation and Auditing of the various information sources involved.

3.1 Security awareness requirements:

- Make participants aware of the risks that threaten the MAZI data and processes, and the toolkit, and the available means of protection.
- Make users aware about information security and train them using the authentication mechanisms in place. Also to understand the related standards and policies and recognise and accept the responsibility for protecting the passwords, smart cards, private keys, etc., by signing the related statements.
- To enhance user's trust in the MAZI toolkit.

3.2 Authentication

The *Regulation (EU) 2016/679 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* requires that any operator who is granted access to sensitive data must be authenticated. Authentication technology should be strict when dealing with sensitive and confidential data available to the users of the platform. To do this, a username and a password will be used so that the person who wants to access the raw data of surveys and interviews confirms that he has authorized access to the system. If deemed necessary by sensitive collected data, which is not currently foreseen in MAZI, we will use an RSA encryption mechanism, with each operator receiving a personal private key.

3.3 Authorization

The objective of the authorization is to determine the rights of a user of an information system. For each researcher, we will specify which content can be accessed based on functionality, security and confidentiality criteria.

3.4 Accounting and Auditing

MAZI should not deal with sensitive data, in any case logging of the personal data will be enforced to prevent abuses, and in case of necessity proper auditing measures as provided by the *Regulation (EU) 2016/679 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* shall be put in action.

4. Conclusions

The deliverable aimed to identify key issues that can arise throughout the life of MAZI regarding ethical issues and management of personal data.

The deliverable first investigated corresponding European directives including Data Protection Directive, e-Privacy Directive. The research conducted in this deliverable includes several important aspects of privacy & data protection from EU regulatory framework and technical perspectives.

The guidelines in the deliverable will be a reference for MAZI partners to be used during its implementation.

5. References

[1] Directive 95/46/EC of 24 October 1995 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 31-50.

[2] Directive 2002/58/EC of 12 July 2002 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal. L 201, 31/7/2002 p. 37-47.

[3] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF)

[4] Chapter 2 Consent & Chapter 4 Privacy and confidentiality: European Textbook on Ethics in Research (2010) Directorate-General for Research, Science, Economy and Society. ISBN 978-92-79-17543-5 http://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

[5] H2020 Programme: Guidelines on FAIR Data Management in Horizon 2020 https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[6] The Charter of Fundamental Rights of the European Union http://www.europarl.europa.eu/charter/default_en.htm

[7] Horizon 2020 ethics self-assessment http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-msca-itn-2015/1620147-h2020_-_guidance_ethics_self_assess_en.pdf

[8] The EU Code of Ethics: http://www.respectproject.org/ethics/412ethics.pdf

ANNEX 1: Example Declaration of Consent for MAZI project

The research activities of the MAZI project include collecting data from participants, within the context of EU-funded research.

You have been invited to participate in the MAZI project and you have received separate information about this activity.

Your data will be held anonymously and used only for the purpose of the MAZI project. It will be stored securely and confidentially until the project activities have been completed. Any written reports or publications referring to your data will not contain any information that could identify you.

Your participation is voluntary, you may refuse to consent or withdraw at any time.

For further information about the MAZI research project, please contact at any time:

……..

Declaration of consent: I hereby give consent for my data to be conveyed and documented for the purpose stated above. I confirm that I have been informed of the nature of MAZI and that my participation is voluntary. I am aware that I may withdraw my consent at any time.

Name: ……..

Signature: ……..

Date: ……..

Signature of MAZI representative: ……..

Please provide your contact information if we are allowed to contact you again with regard to your data. This information will be stored separately from your data.

……

ANNEX 2: Example Confidentiality Agreement

Research data shared between the researchers in the MAZI project may contain personal identifiable information (PII), the usage of which is protected by law. To comply with this law, usage and sharing of data is restricted and it is essential that you follow the guidance and self-assessment procedures defined for MAZI for collecting, processing, sharing and storage of data.

In addition to this you are obliged to comply with the following terms:

- I will not share the participant data collected by the project team with any third parties, including the case study organisations, employers of the participants, or other members of the consortium of the MAZI project without explicit, written consent from the person(s) who provided the data.
- Where relevant, I will instruct the people for whom I have responsibility who have access to the data of the relevant ethical protocols and ensure that they follow the guidelines defined for the project, as listed below.
- I will delete the data at least _____ months after the project outcomes have been published (recommended time is 3 months).

Declaration: I hereby declare my consent with the rules outlined above:

Date:.....

Name & Organisation: .....

Signature: .....

List of persons in my organisation who have access to the data: