Developing metrics and instruments to evaluate citizen science impacts on the environment and society

EC Horizon-2020 Grant Agreement number 824711

Call: H2020-SwafS-2018-2020 (Science with and for Society)

Topic: SwafS-15-2018-2019

Type of action: RIA

Ethics requirements: Protection of personal data

Delivery Year: 2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824711.

Document Information

Project Number	824711			**Acronym**	MICS
Full title	Developing metrics and instruments to evaluate citizen science impacts on the environment and society				
Project URL	**www.mics.tools**				
EU Project officer	Colombe Warin				
Deliverable	**Number**	D6.2	**Title**	POPD - Requirement No. 2	
Work package	**Number**	6	**Title**	Ethics	
Date of delivery	**Contractual**	Month June 2019		**Actual**	Month June 2019
Authors (Partner)	Claire Williams (Earthwatch), Uta Wehn (IHE Delft) and Luigi Ceccaroni (Earthwatch)				
Responsible Author	Claire Williams		**Email**	cwilliams@earthwatch.org.uk	
	Partner	Earthwatch			
Abstract (for dissemination)	This deliverable confirms that a data protection policy for the project will be kept on file. An evaluation of the ethics risks related to the data processing activities of the project is also presented, including an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679. Detailed information on the informed consent procedures in regard to data processing will be kept on file.				
Keywords	Data protection, GDPR, procedures, criteria, informed consent, ethics				

Version Log

Version as date	Author	Partner	Change
2019_03_01	Uta Wehn	IHE Delft	Reference documents from Ground Truth 2.0
2019_06_13	Claire Williams	Earthwatch	Initial document creation and intermediary version for internal reviewers
2019_06_27	Luigi Ceccaroni	Earthwatch	Final review

To cite this document:

Williams, C., Wehn, U. & Ceccaroni, L. (2019). D6.2: Ethics POPD - Requirement No. 2. *Deliverable report of project H2020 MICS (grant agreement No 824711).*

Contents

1 Executive Summary

Humans are not the research subject of R&D activities in MICS. However, participation of humans as citizen scientists is foreseen. In order to facilitate this participation some data will be gathered and so this deliverable confirms that a data protection policy for the project will be followed and kept on file by Earthwatch. An evaluation of the ethics risks related to the data processing activities of the project is also presented, including an opinion on whether a data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679. Detailed information on the informed consent procedures in regard to data processing will be kept on file. The filing location is outlined for the relevant policies and informed consent procedures. This deliverable (D6.2) is to be applied in line with D6.1 regarding the participation of humans.

2 Introduction

The MICS project involves human participants as citizen scientists, through activities such as: data collection, online surveys, focus groups, round tables research, open consultation platform, stakeholder feedback questionnaires, field reports, local-context analysis, retrospective pre-post questionnaires and case studies.

Since these project activities raise a number of ethical issues, this document specifies in detail how the following ethics issue raised in the MICS proposal evaluation (see the following table) will be addressed.

MICS - Ethics Requirement 2	
Ethics Issue Category	Ethics Requirements Description
Protection of Personal Data (POPD)	- The host institution must confirm that it has appointed a *Data Protection Officer* (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be kept on file. - The beneficiary must evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679. The risk evaluation and the opinion must be submitted as a deliverable. - Detailed information on the informed consent procedures in regard to data processing must be kept on file.

This deliverable is to be applied in line with D6.1 regarding the participation of humans.

3 Data-protection host organisation

For the MICS project it has been agreed that Earthwatch, as the Coordinator, will act as host organisation for data-protection purposes.

Earthwatch does not have an appointed *Data Protection Officer* (DPO) in line with the guidance detailed by the UK Information Commissioner's Office, which can be viewed here [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/] and is summarised below:

"Under the GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of lalarge-scalerocessing of special categories of data or data relating to criminal convictions and offences."

Earthwatch confirms the above criteria are not applicable to their organisation. Earthwatch's compliance with data protection regulations is described here: [https://earthwatch.org.uk/privacy-policy].

A copy of the MICS data protection policy will be kept on file in the MICS project internal document shared repository and can be viewed here: [https://mics.tools/privacy-policy].

4 Evaluation of the ethics risks of MICS data processing

4.1 Type of personal data to be collected

For the avoidance of doubt, MICS is primarily concerned with the development of *impact measurement tools.* Humans are not the *subject* of MICS research. Therefore, the MICS tools will collect only citizen-science--project metadata and no personal data. However, humans will *participate* in citizen science case studies during the MICS project to help inform the development of the tools and ensure they are robust. In order to facilitate this participation some personal data will be collected.

The data collected in the MICS project will come from a range of sources, such as workshops, questionnaires, newsletter subscriptions, and registering for the platform. In some cases, the type of data will be personal data as defined by General Data Protection Regulation in Article 4:

> ''any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person''. (GDPR, Article 4, Definitions)

The typical range of personal data will be *name, email address, and photos*. The data will be used in various ways: to enable participation in the citizen science case studies; to keep people informed about the project; and in the case of photos to promote the project activities. Details of the recruitment and informed consent procedures can be found in D6.1 H – Requirement No. 1.

4.2 Data minimisation and processing

According to the General Data Protection Regulation (GDPR), Article 5, "Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".

MICS project data processing will only use as much data as is required to successfully accomplish a given task and will ensure that data collected for one purpose will not be repurposed without further consent.

The MICS project does not involve profiling systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as tracking, surveillance, audio and video recording, geo-location tracking) or any other data processing operation that may result in high risk to the rights and freedoms of the participants.

The MICS project does not involve further processing of previously collected *personal data*, like pre-existing data sets or sources, merging existing data sets.

The processing of the data collected in the MICS project complies with all applicable international, EU and national law (in particular, the GDPR, and national data protection laws).

4.3 Data protection impact assessment consideration

There is a need to consider whether a Data Protection Impact Assessment (DPIA), is necessary for MICS, as defined by General Data Protection Regulation in Article 35:

> "1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

In light of the above, the level of risk must be considered at a high-level to consider whether the DPIA requirement applies. According to the guidance from UK Information Commissioner's Office which can be viewed here [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/] and is summarised below:

> "Risk in this context is about the potential for any significant physical, material or non-material harm to individuals…'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two",

the MICS tools will utilise some of the processing techniques described as "high risk" in guidelines by the working party of EU data protection authorities (WP29), which can be viewed here [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236] and summarised below:

- "Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract."

However (as indicated in sections 4.1 Types of personal data), only citizen-science metadata and **no personal data** will be processed in the MICS tools.

The *personal data* that are collected in the MICS project is minimal (as indicated in sections 4.1 and 4.2 above) and so the likelihood and severity of harm is extremely low.

4.4 Opinion

As detailed above the data captured in the MICS project or tools are unlikely "to result in a high risk to the rights and freedoms of natural persons". Therefore, it is the opinion of the MICS project team that DPIA is not required under art.35 General Data Protection Regulation 2016/679.

5 Informed consent procedures in regard to data processing

The informed consent procedures are detailed in D6.1 H - Requirement No. 1. Detailed information on the informed consent procedures in regard to data processing is detailed below and will be kept on file in the MICS project internal document shared repository.

5.1 General guidelines

In MICS, the following general guidelines for the protection of personal data will be followed:

- The only people able to access data covered by the MICS procedures will be those who need it **for their MICS-related activities**.
- **Mass mailings** to individuals outside the MICS consortium will be sent by including such email addresses in :bcc in order not to disclose the email addresses.
- Personal data **will not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **The MICS partners will provide training** to all their respective team members to help them understand their responsibilities when handling personal data.
- Employees will keep all personal data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords will be used** and they should never be shared.
- Personal data **will not be disclosed to unauthorised people**, either within their own organisation or externally.
- Personal data will be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager if they are unsure about any aspect of data protection.

5.2 Data storage and protection

These rules describe how and where data should be safely stored. When personal data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to personal data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Personal data should be **protected by strong passwords** (e.g. for accessing the electronic device) that are changed regularly and never shared between employees.
- If personal data is stored on removable media (like a CD, DVD or USB sticks), these should be kept locked away securely when not being used.
- Personal data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

5.3 Data retention and destruction

The MICS partners will destroy personal data held when the data are no longer required for the purpose for which they were collected, and when there is no interest to archive them for research and/or statistical purposes. This procedure applies regardless of the format of the data (digital or print).

When there is an interest to archive personal data for research and/or statistical purposes beyond the initially planned data retention period, the personal data will be anonymised to the extent that data users will not be able to identify the individuals concerned.

6 References

- 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)
- UK Information Commissioner's Office Guidance on Data Protection Officer (DPO) requirements - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
- Earthwatch privacy policy - https://earthwatch.org.uk/privacy-policy
- MICS privacy and data protection policy - https://mics.tools/privacy-policy
- UK Information Commissioner's Office Guidance on Data Protection Impact Assessment (DPIA) - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
- Guidelines by the working party of EU data protection authorities (WP29) - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236