YouCount
Youth Citizen Science

D6.2

Data Management Plan

Reidun Norvoll[1]

- Work Research Institute, OsloMet, Oslo, Norway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101005931.

Project acronym	YouCount
Project name	YouCount – Empowering youth and co-creating social innovations and policymaking through youth-focused citizen social science
Grant agreement no.	101005931
Start date of the project	01/02/2021
End date of the project	31/01/2024
Work package producing the document	WP6, Project Management and Ethics
WP leader	Partner 1 OsloMet
Other partners involved	All partners
Deliverable identifier	D6.2
Deliverable lead beneficiary	Partner 1, OsloMet
Internal scientific reviewer(s)	Tomas Kjellqvist, SH; Malin Bruun Kjennerud and Morten Bjørnskau Johannesen, OsloMet (legal consultants)
Due date	July 30, 2021
Date of delivery	Date of submission (to be filled by Coordination Office)
Version	4
Author(s)	Reidun Norvoll (OsloMet) with contributions from consortium partners
Classification	Public

Disclaimer: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No101005931. The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

Table of Contents

List of Figures

List of Tables

Cited as: Norvoll, R. (2021). *D6.2 Data Management Plan. doi. 10.5281/zenodo.5141979*

D6.2 Data Management Plan

This data management plan (DMP) outlines what data will be collected; how research data will be handled during the project and after finalisation; what methodology and standards will be used; whether and how this data will be shared and/or made open; and how the data will be curated and preserved. The DMP is a living document that will be updated throughout the project period as the project evolves.

The vision of YOUCOUNT is twofold, addressing and combining both the scientific and societal needs of our time. The scientific *vision* of YOUCOUNT is to strengthen the transformative and participatory aspects of CS and social science, by enabling citizen participation in all facets, reaching out for a more egalitarian way of conducting science. The societal vision of YOUCOUNT is to contribute to create inclusive and innovative societies for European youths and to empower them in promoting active citizenship and a just and equitable future, particularly for youths with disadvantages.

Table 1. Revision History

Version	Date	Created by	Comments
1.0	18/05/2021	Partner 1, OsloMet	Developed structure and content of the DMP in collaboration with partners
2.0	06/06/2021	Partner 1, OsloMet	Revised DMP after inputs from partners and legal department OsloMet/NSD
3.0	25/06/2021	Partner 1, OsloMet	Revised DMP after scientific review and inputs from GA
4.0	30/07/2021	Partner 1, Reidun Norvoll	Submitted final version 1

Table 2. Terms and Abbreviations

Abbreviation	Full term
AB	Advisory Board
CIS	contact information sheets
CS	citizen science
CSS	citizen social science
CMS	content management system
CCO	Creative Commons Zero
C-YCS	young citizen scientists from the local community or targeted organisation (lower level of participation)
D	deliverable
DEC	dissemination, exploitation and communication
DMP	data management plan
DoA	Document of Action
EB	Executive Board
EC	European Commission
EC-GA	European Commission-Grant Agreement
EU	European Union
FAIR principles	findable, accessible, interoperable, reusable
GA	General Assembly
GDPR	General Data Protection Regulation

ICT	internet communication technology
IP	intellectual property
IPR	intellectual property rights
LL	living labs
NSD	The Norwegian Centre for Research Data
OA	open access
OSc	open science
PEH	Project Executive Handbook
RRI	responsible research and innovation
RT	research team
R-YCS	young citizen scientists participating in the research team
SEB	Safety and Ethics Board
YCS	young citizen scientist
Y-CSS	youth citizen social science
YouCount app	'YouCount CSS app' on the SPOTTERON CS platform
WP	work package
WIC	written informed consent

Executive Summary

YouCount is an EU project funded under Horizon 2020, the Science with and for Society (SwafS) programme. The overarching objective of the YouCount project is to generate new knowledge and innovations to increase the social inclusion of youth through co-creative youth citizen social science (Y-CSS), where young people contribute as citizen scientists and to provide evidence of the actual outcomes of citizen science (CS).

The YouCount project is a large project with a substantial number of participants that requires proper and secure data management throughout the project period and beyond. The data management plan (DMP) outlines what data will be collected; how research data will be handled during the project and after finalisation; what methodology and standards will be used; whether and how this data will be shared and/or made open; and how it will be curated and preserved. Moreover, it sets out how the data management in YouCount will align with the FAIR (findable, accessible, interoperable, reusable) principles.

The DMP also includes relevant legal and ethics requirements, as well as assessments of proper data management in the context of open CSS with youths at risk of social exclusion and how risks can be mitigated.

This first version of the DMP for YouCount comes in the early phase of the project, where many aspects concerning data management have yet to be developed. The DMP will thus be a living document that will be updated on a regular basis and completed as the project evolves.

1 Introduction

1.1 YouCount

1.1.1 Objectives and research questions

The overarching objective of the YouCount project is to generate new knowledge and innovations to increase the social inclusion of youth at risk of exclusion through co-creative youth citizen social science (Y-CSS) and to provide evidence of the actual outcomes of Y-CSS. Multiple case studies—consisting of nine co-creative Y-CSS projects across Europe—will provide increased knowledge of the positive drivers of social inclusion in general and specific knowledge and innovation in relation to social participation, social belonging, and citizenship. The project will include young people from a wide age range: about 13 to 30 years old at the time of recruitment. The project will focus on youth in general but will address the circumstances of youths who are most at risk of marginalisation in terms of poverty, migration, disability, low education, unemployment, and disenfranchisement; some cases will include young people from deprived or disadvantaged areas.

Overall, YouCount targets two strands of inquiry:

- Strand 1. Increased knowledge about positive drivers of social inclusion and new social innovations and policymaking (work package [WP] 2 and 3), including:
    - Which individual, relational, social, and environmental factors contribute to empowerment and increased social inclusion, and why?
    - What kinds of social means and policymaking for social inclusion increase the social inclusion of youths, and why?
- The study also includes three key empirical research questions involving youths:
    - What are young people's views on what the critical issues are for social inclusion?
    - What are young people's experiences with opportunities for social inclusion in their daily lives?
    - What new means and policies for social inclusion do they consider are needed?
- Strand 2. Increased knowledge of Y-CSS for scaling up (WP 1, 3, and 4), including:
    - What should a social scientific framework for co-creative Y-CSS look like?
    - What is the best way to set up co-creative Y-CSS in practice?
    - How can CSS contribute to social innovation?
    - What are the individual, social, and scientific outcomes of Y-CSS?
    - What are the costs and benefits of Y-CSS and the impact of the YouCount project?

1.1.2 Methodological design

The project includes four substudies:

- **Substudy 1.** Development of a framework for Y-CSS
- **Substudy 2.** Implementation of a multiple case study of Y-CSS projects in nine countries across Europe
- **Substudy 3.** Mixed-methods evaluation of the process, outcomes, and impact of the Y-CSS activities, and a multi-criteria assessment of the costs and benefits of Y-CSS
- **Substudy 4.** Creation of social and scientific impact through widespread scaling up and continuity

A transdisciplinary Advisory Board (AB) and Safety and Ethics Board (SEB) with expertise in data protection regulations, ethics, and youth-involved research will follow the project closely during the project period.

Youths will participate as young citizen scientists (YCS) in two ways: Young peoples from the community and university students will participate in the whole research process as citizen scientists (R-YCS) in research teams (RTs). A larger group of young people will serve as community citizen scientists (C-YCS) at a lower level of participation by contributing data about positive drivers of social inclusion on the YouCount Citizen Social Science app (henceforth referred to as the 'YouCount app') on the SPOTTERON Citizen Science Platform. YCS will also provide their perspective on social inclusion and targeted solutions by participating in local dialogue forums (e.g., group conversations or 'listenings'). Each case will establish local living labs (LLs) with multiple stakeholders in the wider community or targeted stakeholder organisations, which will use the data provided by the participating YCS to co-create policymaking and innovations in terms of new ideas, products, and methods to create social change. Some cases will make use of additional data collection methods, such as interviews, small surveys, creative methods, photovoice, and 'splotting'. This is, however, yet to be decided. Our rationale for the choice of a multiple case study is that adoption of this design allows for contextualised and holistic research and innovation by exploring a real-life contemporary bounded system (a case) and multiple bounded systems (cases) over time through detailed, in-depth data collection involving multiple sources of information. This will provide detailed and dynamic information about the multifactorial and interactive drivers of social inclusion.

The evaluation and impact study will include a combination of quantitative and qualitative measures. Given the complexity of the research field of social inclusion and the limitations of sampling and resources, we consider randomisation to not be the best option; rather, a holistic evaluation based on a multiple case study approach that allows for contextualised and cross-case

analysis of outcomes and 'thicker descriptions' of factors and mechanisms that might contribute to the various outcomes on an individual, reciprocal, and social level, is the more optimal choice. The outcome study of Y-CSS will be based on pre–post measures of a defined set of indicators (or variables) according to the overarching research framework. The exact variables and choice of questionnaires have yet to be decided. Moreover, the evaluation study will also include a formative evaluation strategy that will allow assessments of the quality and effectiveness of the ongoing project and will inform changes that may improve the project. In doing so, we will combine a standardised approach (i.e., all projects will rely on the same questionnaires and evaluation grids) with an open approach (i.e., evaluating each project individually, employing qualitative interviews that allow for in-depth insights into how citizens experience participation and into the mechanisms behind outcomes). Most importantly, we will also involve the Y-CSS in the evaluation process; that is, citizen scientists will evaluate the ongoing project and its outcomes (WP 4).

In view of language challenges and diverse local contexts, the multiple case study and evaluation study will be conducted on the national level, where the national RT (consortium partners) will prepare the study by translating the cross-case questionnaires and interview guides into the native language, conduct the interviews and questionnaires in practice, and then write case reports in English and on the cross-case level. UNVIE will coordinate and conduct the evaluation study. The combination of WP 2, 3, and 4 will provide opportunities for contextual and comparative analysis. The established relationships with the field through WP 2 may decrease the risk of non-participation.

The final choice of data collection methods will be decided during 2021/2022 and integrated into the DMP.

1.2 The YouCount DMP

The YouCount project adheres to the principles of responsible research and innovation (RRI) and open science (OSc), as promoted by Open Research Europe and EU Horizon Europa. YouCount is part of the Open Data Research Pilot (ODR-Pilot). This participation comprises the EU requirements as set out in the Horizon 2020 EU-GA, Article 29 (page 252) for developing a DMP as a deliverable of the project within the first 6 months of the project implementation and for storing open data in a suitable repository.[1]

[1] European Research Council (ERC). Guidelines on Implementation of Open Access to Scientific Publications and Research Data in projects supported by the European Research Council under Horizon 2020. Version 1.1. 21 April 2017. h2020-hi-erc-oa-guide_en.pdf (europa.eu)

The aim of this DMP is thus to outline how data will be collected, processed, and generated in the YouCount project during the project period and after finalisation. The DMP will align with the FAIR principles of making data findable, accessible, interoperable, and reusable. In addition, the DMP will provide information on the measures taken to safeguard and protect sensitive data and how the DMP will be integrated with the choice of trustworthy open repositories.[2]

This version of the DMP for the YouCount project comes at an early stage of the project, where many details of the project design have yet to be developed. The DMP thus only outlines the basic principles for data management in the project and will be updated on a regular basis throughout the project period as the project evolves. The project has established a DMP group consisting of representatives from each partner (see Table 4) who will revise and update the plan when changes occur (e.g., new data sets, changes in consortium policies) and at least every ninth month in relation to EU and internal reporting.

The DMP for YouCount complements and reuses key elements of the ethics requirements and procedures, as set out in related deliverables during 2021. These are: D6.6 Report on the Recruitment Criteria and Informed Consent Procedures, and D7.1 POPD Requirement No. 2, submitted by July 31. D2.1 which will be submitted by December 2021, will describe the established collaboration with the ethics board, securing of formal ethics approvals at the local level, and final consent letters. See also D6.1 Project Executive Handbook (PEH) and D6.3 Intellectual Property Rights (IPR) Plan for further details of the project's procedures and guidelines regarding data management and OSc (data and publications).[3]

1.3 Relevant work packages for the DMP

As discussed above, the YouCount project is a large project with a substantial number of participants that requires proper and secure data management throughout the project period and beyond. The overall and specific objectives for the project are detailed in six work packages (WPs):

[2] Science Europe: Practical guide to the international alignment of research data management. Extended Edition. (2021), se_rdm_practical_guide_extended_final.pdf (scienceeurope.org)
[3] Norvoll, R. and Nedberg, H. (2021). *YouCount. D.6.3 IPR plan*. Zenodo. doi.10.5281/zenodo.4720474.

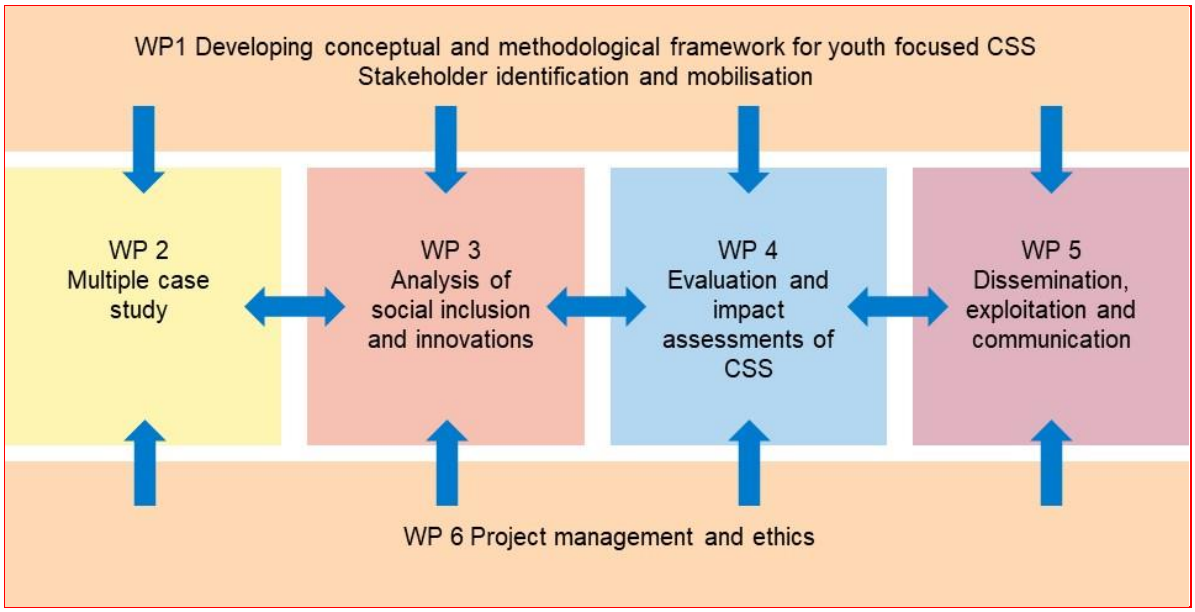

Figure 1. Interrelations between the six YouCount work packages (WPs).

As seen in Table 3, the YouCount consortium will be engaged in data collection and data management in several WPs and substudies.

Table 3. Overview of Data Collection in Each Work Package (WP) and the Methods and Partners Involved

Research issue	WP	Methods	Partners involved
Developing framework & stakeholder mobilisation	WP 1	Reviews, webinars, internet list of stakeholder organisations on project webpage	KTU, SPOTTERON, OsloMet VA, SH, UCLan, FD, UNIVIE, AAU, ESSRG, UNINA
Multiple case study: Implementation of Y-CSS	WP2 & 3	Mixed-methods design: Field work and training of R-YCS. Systematic recording of RTs' experiences with setting up Y-CSS and self-evaluation	OsloMet, VA, SH, UCLan, FD, UNIVIE, KTU, AAU, ESSRG, UNINA
Multiple case study: Positive drivers of social inclusion	WP 2 & 3	Mixed-methods design: Field work, dialogue forums/focus groups, participatory observation LLs, YouCount app, national workshops	OsloMet, VA, SH, UCLan, FD, UNIVIE, KTU, AAU, ESSRG, UNINA, SPOTTERON

		Additional: interviews, 'splotting', photovoice, survey	
Evaluation study: Process and outcomes of Y-CSS		Mixed-methods design: Pre–post survey and focus group- as well as individual interviews with project participants (researchers and R-YCS) and stakeholders in community/organisations Online expert panel meeting and ECSA workshop (external evaluation)	UNIVIE OsloMet, VA, SH, UCLan, FD, KTU, AAU, ESSRG, UNINA, SPOTTERON
Evaluation and impact study: Costs/benefits and impact assessments	WP 4	Multi-criteria framework assessments based on conversations with the RTs, data from WPs, and secondary data concerning project outputs	FD OsloMet, VA, SH, UCLan, UNIVIE, KTU, AAU, ESSRG, UNINA, SPOTTERON

1.4 Members of the YouCount DMP group

Each partner has appointed the following responsible persons as presented in Table 4.

Table 4. Overview of the Members of the YouCount DMP Group

Partner	Name
OsloMet	Reidun Norvoll
VA	Fredrik Brounéus
SH	Ann Mutvei Berrez

UCLan	Deborah Crook
FD	Susana Franco
UNIVIE	Isabelle Freiling
KTU	Raminta Pučėtaitė
AAU	Michael Søgaard Jørgensen
ESSRG	György Pataki
UNINA	Fortuna Procentese
SPOTTERON	Philipp Hummer

1.5 DMP definitions

This section provides definitions of the key concepts used in the DMP.[4]

Personal data: Any data that can be linked to an individual natural (physical) person. This includes objective information, such as a person's age, name or e-mail/IP address, national ID number or annual income, or voice on a sound recording. However, personal data can also have a more prosaic nature. Moreover, it is important to distinguish between directly and indirectly identifiable personal data, where the information provided makes it possible to identify one or more people. The extent to which background information can make a person identifiable depends on the variables/registered data as well as the context, topic, and sample criteria.[5]

Sensitive data: Includes information regarding a person's racial or ethnic origin; political, philosophical, or religious views; health issues; sexual relations; membership in a trade union; or history of being suspected, charged, indicted, or convicted of a criminal offence (Article 9(1) GDPR). Like other co-creative CSS projects (e.g., the CoAct project[6]), the nature of the YouCount project focusing on the social inclusion of youths at risk of exclusion will include moments where

[4] Please see Notification Form for personal data | NSD or https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/anonymisation/glossary/
[5] EUR-Lex - 32018R1725 - EN - EUR-Lex (europa.eu)

[6] Lombion, Cédric (2020). CoActD1.2: Data Management Plan. Zenodo. http://doi.org/10.5281/zenodo.4498287

the YCS might share their personal perspectives on the topic of the research. This can create two types of situations wherein personal or sensitive data is generated and collected: first, situations in which the academic researcher *will* collect personal data for analysis purposes, and second, situations in which the academic researcher does not aim to collect these types of data, but personal or sensitive data *may* come up during the research and innovation activities. Approaches to handling these types of data are described below.

Non-personal data: Includes all data not covered by the above definitions, such as aggregated data, anonymised data, and open government data.

Anonymous data[7]: Data that is impossible, using all reasonable technical means, to link back to an individual natural person. When personal data is anonymised, it is no longer deemed to constitute personal data. The principles of data protection should not concern the processing of such anonymous information, including for statistical or research purposes.[8]

Anonymisation: The process of rendering data into a form in which it is no longer possible to identify individuals and where the risk of identification does not exist using all reasonable technical means. Anonymisation is about removing the possibility of identifying individuals in a data set. Anonymisation is an important means of enabling the extraction of valuable insights through data analysis while reducing the risks for those concerned. However, the increased risk of reidentification means that it is important to perform thorough risk assessments before publishing anonymised data and to use robust anonymisation techniques. A thorough and transparent anonymisation process is therefore part of risk mitigation and secure data processing in the YouCount project. Recommended guidelines for anonymisation, as provided by data protection bodies, will be used before the data is made openly available.

De-identification: The removal of all uniquely personal characteristics from the data so that they can no longer be linked to a specific individual. This term is now often integrated with pseudonymisation.

Pseudonymisation: A process whereby directly identifiable parameters are replaced by unique indicators to conceal the real identities of the data subjects. This can be fictive names or a 'key code', also called 'scrambling code', for each person. According to GDP, personal data that has undergone pseudonymisation but could be attributed to a natural person using additional information should be considered information on an identifiable natural person. Pseudonymisation is thus not intended to preclude any other measures of data protection.[9] However, pseudonymisation is regarded as a powerful measure for reducing the risks to the data subjects concerned and helping controllers and processors to meet their data protection

[7] The anonymisation of personal data | Datatilsynet
[8] EUR-Lex - 32018R1725 - EN - EUR-Lex (europa.eu)
[9] EUR-Lex - 32018R1725 - EN - EUR-Lex (europa.eu)

obligations. In the YouCount DMP, personal data that has undergone pseudonymisation but could still be attributed to a natural person using additional information will thus be treated in a confidential way. To determine whether a natural person is identifiable, we will consider all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.[10]

Primary and secondary data: Primary data refers to the first-hand data gathered by the researcher themself. Secondary data refers to data collected by someone else earlier.

Data processing: Any operation performed on personal data. Processing can include collecting and registering, arranging and analysing, transferring and storing, or publishing and archiving. Processing refers to everything you "do" with data.

Data controller: The organisation or person who determines how and for what purpose personal data is to be processed. The data controller is responsible for ensuring that the data is processed in accordance with the GDPR.

Data processor: The organisation or person who processes personal data on behalf of the data controller, and only as specifically agreed with the data controller.

1.6 Structure of the DMP

The DMP is inspired by the overall requirements for DMPs as set out by Science Europe (Science Europe, 2021)[11] but is mainly structured according to the DMP template of Horizon 2020. In addition, we used the interactive data management template provided by the Norwegian Centre for Research Data (NSD) as a support during the work since this template aligns with the EU requirements and is connected to the obligation to submit a notification form to the NSD for OsloMet as project coordinator and data controller for the YouCount project.[12]

Subsequently, the following DMP for YouCount will be divided into eight main chapters: 2) Ethical and legal requirements; 3) Data summary; 4) FAIR data; 5) Allocation of resources; 6) Data security; 7) Ethics aspects; and 8) Other issues.

[10] EUR-Lex - 32018R1725 - EN - EUR-Lex (europa.eu)
[11] se_rdm_best_practices.pdf (scienceeurope.org)
[12] Create a data management plan | NSD

2 Ethical and Legal Requirements

The protection of natural persons in relation to the processing of personal data is a fundamental right.[13] The YouCount project will thus adhere to relevant guidelines and codes for good conduct of research. All partners have also started their commitment to secure confidentiality and good ethical conduct of research as part of the Grant Agreement (EC-GA), Consortium Agreement (CA), and PEH, including:

- The Nuremberg Code (1947) addressing volunteer consent and proper acting.
- The European Legal Framework, including its ethical standards and guidelines.

Furthermore, the consortium will comply with relevant EU legislation for human studies, including:

- The Declaration of Helsinki in its latest version.
- The Charter of Fundamental Rights of the EU (2000/C 364/01).
- The New Brunswick Declaration: A declaration on research ethics, integrity, and governance resulting from the 1st Ethics Rupture Summit, Fredericton, New Brunswick, Canada (2013).
- The Respect Code focused on socio-economic research (www.respectproject.org).
- The European Code of Conduct for Research Integrity (https://allea.org/code-of-conduct/).
- Regulation (EU) 2016/679 of the European Parliament and Council (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; GDPR).

The project will also fully comply with the Norwegian Personal Data ACT (2018), the Norwegian National Research Ethics Committee's ethical guidelines to protect individuals involved in research, the European legislation and fundamental ethical principles, reflected in the Charter of Fundamental Rights in the EU, and the European Convention on Human Rights and its Supplementary Protocols. All aspects of data protection will also be approved by the national bodies responsible for protecting personal data and in accordance with Article 8(3) of the Charter of Fundamental Rights of the EU.[14]

As elaborated below, the project will adhere to regulations and ethical guidelines concerning potential vulnerable groups and underaged participants in research in the participating case countries, and European legislations. In general, most YCS will be above 18 years of age. However,

[13] Regulation(EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC EUR-Lex - 32018R1725 - EN - EUR-Lex (europa.eu)

[14] Data protection in the EU | European Commission (europa.eu)

at least five of the nine cases will include some youths aged 13–18 in the research teams (R-YCS) or as C-YCS providing data in dialogue forums and on the YouCount app (cf. D7.1 POPD requirements No.2).

When it comes to the question of children's legal capacity to consent to processing of their personal data, GDPR Article 8(1) regulates that children's personal data can be lawfully processed by information society services based on children's consent when the child is at least 16 years old. Below that age, such processing based on consent is only lawful if consent is also given or authorised by the child's parents. Member states to the EU/European Economic Area (EEA) might, by law, provide for a lower age for the legal capacity to consent, but not below the age of 13 years. GDPR Article 8(2) also points out that GDPR Article 1 only regulates the question of children's legal consent in relation to information society services. Article 8(2) states that the regulation in Article 8(1) does not affect the general contract law of Member States, such as the rules on the validity, formation, or effect of a contract in relation to a child. EU/EEA Member States and the UK may have a variety of rules regarding children's legal capacity to enter various types of contracts. The main rule in all these countries is probably the age of maturity for entering legal binding contracts, although exceptions exist in all these countries regarding this starting point/main rule.

Subsequently, the regulation in GDPR Article 8 regarding information society services does not apply to a child's consent to data processing in other contexts or for other purposes, such as participation in research. The question of the legal capacity of children to consent to data processing and research participation is not regulated specifically in the GDPR. The age threshold for obtaining parental consent to research varies between 13 and 18 years, depending on the age established in each EU Member State. These variations in age threshold also apply for the consortium partners participating in YouCount (cf. D7.1 POPD requirement No.2). It will thus be necessary to adhere to each partners' national data protection authority.[15] Further, the GDPR Recital 38 provides for guidance regarding ethical considerations:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of children's personal data for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Those interested in using children's personal data must provide a proportionality test, considering and weighing the aim of data processing and positive outcomes against the possible harm the use of personal data might have on children.

[15] Can personal data about children be collected? | European Commission (europa.eu)

The project coordinator has submitted a first notification about the project to the NSD (serving OsloMet), which will function as the lead supervisory authority for the project. The NSD has assessed that the age limit for parental/guardian consent is 15 years of age in the YouCount project if not collecting sensitive/health data. For those under 15 years of age, parental/guardian consent is required. However, the needs for parental/guardian consent will depend on the kind of collected data, the sensitiveness of the data, the level of participation, and national regulations and will, therefore, be finally decided together with the NSD and national supervision authorities as part of the data protection/ethic approval process when the data collection methods are more detailed.

Moreover, Norway (Coordinator) and the UK (University of Central Lancashire [UCLan]) are non-EU country consortium partners during the project period. Although not a member of the EU, Norway is a member of the EEA. The GDPR was incorporated into the EEA agreement and became applicable in Norway on 20 July 2018. Norway is thus bound by the GDPR in the same manner as EU Member States. As of 1 February 2020 ("the withdrawal date"), the UK is no longer a member of EU. During the transition period, the GDPR continued to apply to and in the UK as if it were a Member State.[16] This transition period ended June 2021.[17] On June 27, 2021, it was decided by the EC that the UK had an adequate level of protection for personal data. This means that personal data can be transferred to the UK without additional obligations, even if the UK is no longer part of the EEA. YouCount will comply with EU data protection rules and meet all national requirements for partners in relation to data collection and data processing of personal data that will be collected on the national level. The project will ensure that transfer of personal data is transferred from EU to non-EU countries in accordance with Chapter V of the GDPR 2016/679.

[16] Regulations | Datatilsynet https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en (retrieved on 17. April 20209. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en (retrieved on 17. April 2020) and data_protection_en.pdf (europa.eu))

[17] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/eu-kommisjonen-med-adekvansbeslutning-for-storbritannia/

3 Data Summary

In sum, data collection, generation, and processing in the YouCount project serve two main purposes, as outlined in the project objectives and research questions above: first, to support the research activities and validate research results, and second, to support communication with project stakeholders and contribute to build and scale up (Y-)CSS.

3.1 Types and formats of data

The data collected and generated in the YouCount project reflects the mixed-methods project design and will consist of several types and formats.

3.1.1 Data types

In general, the data types will consist of:

1. Non-personal data based on anonymous transcripts of interviews/dialogue forums, summarised case reports, and data collected for statistical purposes and generated through automated analysis and for open data manually checked and quality assured before publication
2. De-identified/pseudonymised types of qualitative and quantitative data
3. Directly identifiable personal data (name, contact information) to be used for internal communication in the research teams, among participants in the case study, or in promoting the case study in dissemination, exploitation, and communication (DEC) activities
4. Potentially indirectly identifiable personal data due to small samples (e.g., LLs) that will need closer assessment/procession and, if necessary, new informed consent
5. Sensitive data that might occur spontaneously during conversation

Moreover, the data can be split into raw data, which includes direct personal data (e.g., name lists and audio recordings), and processed data, where personal data has been anonymised or de-identified/pseudonymised. In YouCount, the raw data will be kept on the case/researcher level, and processed data transferred.

Textual data: Most data will take form as text in terms of minutes, summaries, transcripts, field notes, templates for recording events, and comments provided by YCS on the YouCount app.

Tabular data: This will consist of aggregated and anonymised data based on quantitative data collection undertaken in WP 2, 3, and 4 using questionnaires and the YouCount app. See Figure 2 for an example of exported CSV files from the app (presented here without user ID numbers).

Image data: Image files for research illustration and in user generated data. YCS can upload pictures to the YouCount app attached to data points (in line with GDPR). Based on informed consent, personal identifiable pictures taken by researchers on institution smartphones to illustrate hands-on Y-CSS (e.g., training sessions with R-YCS will be used as illustration). We are also considering the possibility of recording some training sequences. The use of photovoice in some cases has yet to be finally decided.

Audio data: This will mainly be in terms of the use of an audio recorder during interviews. Currently, the actual use of an audio recorder and transfer from audio recorder to PC is unknown and must be followed up through new notifications to supervisory authorities at OsloMet and in each case country. In many cases, researchers might only write pseudonymous/anonymous summaries from the interview/dialogue before deleting the recording on the audio recorder. Possible recording of training sessions and so forth will include audio data.

Other: Interactive data (between YCS) on the YouCount app, online forum for YCS across countries (if accepted by the R-YCS), and presentation of stakeholder organisations on the project webpage.

3.1.2 Format and software

As of now, the data formats will include DOCX, PDF, JPG, XLS, CSV, SPW, and SAV, and Mplus for structural equation modelling (SEM) analyses. The latter works with data files (.dat), input files (.inp), and output files (.out), which can all be opened with the Notes app for Windows after the analyses have been run.

The software used will include MS Word, Joomla Content Management System (CMS), MS Outlook, SPSS, MPLUS, Qualtrics, MaxQDA, ATLAS.ti, and maybe NVivo.

Data on the project home page will be stored as SQL (database), and exports of data from the YouCount app to the Administration Group (the project coordinator and related WP leaders) as CSV.

ID,ROOT_ID,LATITUDE,LONGITUDE,SPOTTYPE,IMAGE,CATEGORY,SUBCATEGORY,OTHER,OTHER_LOCATION,LOCATION_GENRE,DESCRIPTION,STYLE,LOCATION,CREATOR_CHECK,SPOTTED_AT
2451,2451,48.202391,16.354003,„https://files.spotteron.com/images/spots/000004/2015/07/2c6b87dbb9-1435941582188.jpg,Wallart,„„@magnificentmagnus,„false,"2015-07-03 15:40"
2452,2452,48.20226,16.353959,„https://files.spotteron.com/images/spots/000004/2015/07/c13f20025e-1435941694439.jpg,"X Tags",„„fatcap,„false,"2015-07-03 15:42"
2453,2453,48.202281,16.353027,„https://files.spotteron.com/images/spots/000004/2015/07/ecdcb26b59-1435941822233.jpg,"X Tags",„„"Door with tags",fatcap,„false,"2015-07-03 15:44"
2454,2454,48.201564,16.351317,„https://files.spotteron.com/images/spots/000004/2015/07/ee7a8ae9cd-1435942022175.jpg,"Poster & Pasteup",„„"Social message included. Worn down over time",„false,"2015-07-03 15:4
2455,2455,48.201032,16.350312,„https://files.spotteron.com/images/spots/000004/2015/07/0d75870daa-1435942200699.jpg,Throw-Up„„"old Graffiti",blockbuster,„false,"2015-07-03 15:50"
2456,2456,48.200567,16.350447,„https://files.spotteron.com/images/spots/000004/2015/07/883ac2142d-1435942330474.jpg,"X Tags",„„„false,"2015-07-03 15:52"
2458,2458,48.200395,16.350662,„https://files.spotteron.com/images/spots/000004/2015/07/cd44c5849b-1435944546887.jpg,Stencil,„„Stencil,„false,"2015-07-03 16:29"
2459,2459,48.201513,16.350461,„https://files.spotteron.com/images/spots/000004/2015/07/08082427c0-1435944701271.jpg,Sticker,„„character,„false,"2015-07-03 16:32"
2460,2460,48.204188,16.353843,„https://files.spotteron.com/images/spots/000004/2015/07/fa3585c135-1435945936551.jpg,Sculpture,„„"2 cent StÃ¼ck auf Kaugummi",„false,"2015-07-03 16:52"
2462,2462,48.211323,16.33929,„https://files.spotteron.com/images/spots/000004/2015/07/f2e9ce524f-1435963307989.jpg,Piece,„„character,,false,"2015-07-03 21:42"
2463,2463,48.2108,16.339006,„https://files.spotteron.com/images/spots/000004/2015/07/b1c17bc151-1435968537047.jpg,"X Tags",„„"At rhiz",fatcap,„false,"2015-07-03 23:09"
2464,2464,48.210949,16.341057,„https://files.spotteron.com/images/spots/000004/2015/07/0ea28f4e63-1435981684257.jpg,Throw-Up„„„false,"2015-07-04 02:48"
2466,2466,48.210228,16.345233,„https://files.spotteron.com/images/spots/000004/2015/07/3f02718522-1435982231388.jpg,Sticker„„„object,false,"2015-07-04 02:57"
2467,2467,48.209685,16.347925,„https://files.spotteron.com/images/spots/000004/2015/07/fe3a32deac-1435982433538.jpg,"X Tags",„„"Fast cap tag 2014",fatcap,wall,false,"2015-07-04 03:01"
2468,2468,48.20893,16.350494,„https://files.spotteron.com/images/spots/000004/2015/07/af53d74615-1435982678746.jpg,"X Tags",„„"Streetart auch?",„object,false,"2015-07-04 03:05"
2469,2469,48.208644,16.350665,„https://files.spotteron.com/images/spots/000004/2015/07/dc39858034-1435982770264.jpg,"X Tags",„„blockbuster,„false,"2015-07-04 03:06"
2470,2470,48.208372,16.350644,„https://files.spotteron.com/images/spots/000004/2015/07/f5845bef77-1435982851235.jpg,Graffiti,„„„false,"2015-07-04 03:08"
2471,2471,48.208186,16.350537,„https://files.spotteron.com/images/spots/000004/2015/07/dd0b527954-1435982970050.jpg,Stencil,„„"Antifa Graffiti",„false,"2015-07-04 03:09"
2472,2472,48.207795,16.352753,„https://files.spotteron.com/images/spots/000004/2015/07/064373e4b3-1435983152119.jpg,"X Tags",„„fatcap,„false,"2015-07-04 03:13"
2473,2473,48.206504,16.35402,„https://files.spotteron.com/images/spots/000004/2015/07/2998ca354b-1435983340580.jpg,Throw-Up,„„Eo,silver,„false,"2015-07-04 03:16"
2474,2474,48.206075,16.354105,„https://files.spotteron.com/images/spots/000004/2015/07/e8700da709-1435983417185.jpg,"X Tags",„„„false,"2015-07-04 03:17"
2475,2475,48.204912,16.354441,„https://files.spotteron.com/images/spots/000004/2015/07/20131af3de-1435983614061.jpg,Sticker„„Collage,,object,false,"2015-07-04 03:20"
2476,2476,48.302517,16.360697,„https://files.spotteron.com/images/spots/000004/2015/07/8284be9b99-1436025329223.jpg,"X Tags",„„"Crossed Joe",fatcap,wall,false,"2015-07-04 14:55"
2477,2477,48.203051,16.357371,„https://files.spotteron.com/images/spots/000004/2015/07/8877cb1773-1436064487370.jpg,"X Tags",„„"Tag im MQ",„false,"2015-07-05 02:48"
2480,2480,48.203618,16.356888,„https://files.spotteron.com/images/spots/000004/2015/07/2e1d4d710a-1436068578456.jpg,Sticker„„„wall,false,"2015-07-05 02:56"
2481,2481,48.20405,16.356524,„https://files.spotteron.com/images/spots/000004/2015/07/937ae6d1fb-1436068713303.jpg,"X Other",„„"zur heiligen dreieinigkei,
Atelier",„false,"2015-07-05 02:59"

Figure 2. Example of exported CSV data files from SPOTTERON apps (ArtSports – open data).

3.1.3 Language

The data will comprise 11 languages.

The consortium will use English as the main communication form. Summary case reports will be written in English to allow for cross-case analyses. Each country will use their national language during their local case study (English, Norwegian, Swedish, Danish, Lithuanian, Austrian German, Italian, Spanish, Hungarian, and respectively). In addition, Arabic and French will be used when necessary for communication with YCS. Sign translation will be used for youths with hearing disabilities.

3.1.4 Participants (sample)

The groups of participants (sample) that will provide data for the project include:

- Researchers in each case study

- Young people (about 13-30 years of age at the time of recruitment), either as R-YCS or C-YCS
- Local stakeholders participating in the local living labs (LLs; e.g., community administrators, policymakers, social workers, local social entrepreneurs, local influencers , youth council/centre, NGOs, youth/migrant organisations) or local stakeholders that will be included in the evaluation study (outcomes of the case)
- National stakeholders: policymakers, public authorities, NGOs, stakeholder organisations, academics, universities, etc.

Exact numbers are still unclear and will depend on the size of LLs and recruited youths. For now, we calculate that each case will have about 2–5 researchers, 10–15 R-YCS, 15 member LLs, 30–50 participants in national workshops, and 20–100 community youths participating in dialogue forums and providing data on the YouCount app. In total, we estimate approximately 150–170 participants in each of the nine case studies, for a total of about 1400 participants.

3.1.5 Data packages

The legal basis for collecting data and personal data in the data packages is GDPR Article 6(1)(f) Legitimate Interest (data package 1, WP1 Internet list) and GDPR Article 6(1) Informed Consent.

The data collection framework is under development. The basic features of the YouCount app have yet to be completed and will be further developed and designed together with partners and youth organisations/YCS in autumn 2021.

Table 5. Overview of Data Packages, Kinds of Data, and Data Processing in YouCount

Data package	Kinds of data	Confidentiality level	Storage	Sample size	Transfer*
1. WP 1 Developing framework and stakeholder mobilisation: Internet list stakeholders	Contact information sheets (CIS)/written informed consent (WIC) Text description of	Open Internal	Project webpage MS Teams project platform	30–50	Textual data Tabular (CSV)

	stakeholder organisation Optional: Contact information		(private channel/ marked confidential)		
2. WP 2 & 3 Multiple case study: Implementation of Y-CSS	CIS/WIC Texts: Minutes, transcripts, field notes, self-assessment forms, writings or diaries Photos, maybe recordings Audio recording Content coding Compilation/ Synthesis	Confidential (personal data), internal or open May be sensitive data	Secure area: PC – Common/ shared area, institution/ local disk, institution Multifactor authentication OsloMet Teams on OneDrive/ Share Point Smartphone/ tablet, institution External hard drive (etc.), institution	Nine case countries × approx. 20 researchers /R-YCS	Textual data: Text notes, CIS/WIC Photo/ recordings Audio files (ZIP files)
3. WP 2 & 3 Multiple case study: Positive drivers of social inclusion	CIS/WIC Texts: Transcripts, minutes, field notes, self-assessment forms, writings, or diaries Audio recordings	Confidential (personal data), internal or open May be sensitive data	See above, data package 2 Maybe TSD (OsloMet)	150–180 C-YCS 900 R/C-YCS or as many as possible 150–180 stakeholders LLs	Textual data: Text notes, CIS/WIC Photo/video files. Maybe tabular

	Maybe interview, 'splotting', photovoice, self-administered questionnaire Summary, Content coding, Compilation/ Synthesis				
4. YouCount app SPOTTERON CS platform (WP 2, 3, & 4)	GIS data Text: On platform or as summaries Pictures: On platform Statistics: On platform, CVS Content coding, Compilation/ Synthesis	Confidential (applied user privacy/informed consent)[18] Open data (manually checked) Internal (data analysis, including user ID numbers)	All data is stored by SPOTTERON De-identified exported CVS files stored at case partner institutions and OsloMet Open data: open data repositories (e.g., Zenodo), project webpage	900 R/C-YCS or as many as possible	Open data Textual data Tabular data (CVS files) Protected by industry-standard encryption via Transfer Layer Security (TLS/SSL)
5. WP 2 & 3 Multiple case study: CSS as a way to social innovations	CIS/WIC Texts: Transcripts, minutes, field notes, self-assessment forms	Confidential (personal data), internal and open	See above, data package 2 and 3	Approx. 70 (researchers, R-YCS, stakeholders LLs) × 9 = 630	Textual data: Text notes, CIS/ WIC Tabular files?

[18] See https://www.spotteron.net/citizen-science-app-features/privacy-data-safety. On all apps, users can find options to export a copy of all their personal data directly and to anonymise all their personal information

and policymaking	Photo (illustration) Audio recording Summary, Content coding				Photos?
6. WP 4 Evaluation study: Process and outcomes of Y-CSS	CIS/WIC Texts: Transcripts, field notes, self-assessment forms Statistics: YouCount app, questionnaire Audio recordings Content coding, Compilation/ Synthesis	Confidential (personal data), internal and open	See above, data packages 2, 3, & 4	Approx. 27 focus groups with RTs, R-YCS, stakeholder LLs + external stakeholders × 10 = 200–250 Interviews on top as needed Pre–post survey: Approx. 900 YCS if all take part × 2 Number of self-reports unknown	Textual data: Text notes, CIS/WIC Tabular fields Transcripts/ audio files (ZIP files)

7. WP 4 Evaluation and impact study: Costs/benefits and impact assessments	CIS/WIC Texts: Transcripts, minutes, field notes, self-assessment forms, writings, or diaries Maybe audio recordings Summary Content coding	Confidential, internal and open	See above	Maybe approx. 20 (RTs including R-YCS) × 9 = 180 Secondary project output data from all WPs	Textual data: Text notes, CIS/WIC Audio files (ZIP files)

*Dependant on confidentiality level/GDPR

3.1.6 Data minimisation

According GDPR Article 5(c), which addresses principles relating to processing of personal data, personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

As described above, the YouCount project will collect a minimum of personal data (referring back to an individual natural person) in the project, except for name and contact information for practical research reasons (e.g., WIC, ‘scrambling key’ pre–post survey) and personal data related to DEC activities if the participants want to promote the case or themselves.

Personal research data will be immediately anonymised or pseudonymised by the data controller/processor in charge of the data collection. If sensitive data is revealed spontaneously during conversations, it will be deleted or not written down or written down in an anonymous way if the data contributes to answering the research question. If immediate deletion is not possible, the data will be stored on secure servers for sensitive data.

The YCS participating in the YouCount app will provide e-mail addresses, usernames, and IP addresses when signing up (disclosed for all other than SPOTTERON). The app includes functionalities such as the right to erasure and data protection by design. On the platform, users

can find options to export a copy of all their personal data directly and to anonymise all their personal information stored on the SPOTTERON servers. The app allows users to upload open personal identification (username, pictures) or be totally anonymous; this is totally user-led. Advice regarding balancing openness with caution is included in the terms of use. At this stage, we will advise the participating youths to use fictive usernames, avoid sharing personal photos, and hide GIS data that discloses personal and sensitive information to minimise the amount of personal data shared. Still, some YCS might want to use their real names to contact other youths on the interactive platform (peer support). The use of fictive vs. real names must thus be considered together with the YCS and according to WIC at a later stage. User account data as platform-specific data is not shared in data export (CSV files) beside a de-identified user ID number. There is a strict separation of platform-specific data, such as user accounts, and project-specific data, such as answers to implemented questionnaires, for creating new data points in the app during the project. Only project-specific data is shared with the project in line with the SPOTTERON terms of service/partner agreement (https://www.spotteron.net/partner-agreement), except such data to which participants have provided their informed consent before for a specific purpose (e.g., for subscribing to the project newsletter).

The stakeholder organisations and contact persons participating in the LLs (or national workshops) may be publicly known according to informed consent, especially at the local case level. Some stakeholders and R-YCS participants might also want their participation to be known publicly as part of local work, to promote their innovative work as a community/organisation, or for use in their personal CV. Still, the researchers will avoid referring data back to a single person and will keep data as anonymous as possible. Since the RTs and LLs will be small groups, the risk of indirectly recognisable data must be addressed in a proper way and according to informed consent.

Personal data referring to a natural person will be stored for as short time as possible and deleted shortly after the end of the project. The length of storage for each substudy will be included in the WIC.

3.1.7 Origin and reuse of the data

The data analysis and project results will generally be based on primary data from the case studies. In addition, secondary data in terms of project outputs, reviews of scientific and grey literature, internet sites (e.g., CS projects), and other kinds of desk research will be used.

The project might also reuse related open data provided by other CS projects in open repositories for comparison or complementary data during the analysis and publication of findings.

3.1.8 Expected size of the data

As seen in sections 3.1 and 3.2, the data processed by the YouCount consortium will be collected in a variety of formats. The actual size of the data is unknown but is expected to reach 1–2 terabytes in size by the end of the project.

3.1.9 Data utility

As seen from the D5.7 DEC Plan[19] and sections 3.1.4 and 3.1.5, the data in the YouCount project will include a broad potential user group, including stakeholder groups, academic communities, mutual learning processes with CS projects in the EU SwafS programme, research councils and science communications institutions and organisations, university institutions (formal education), CS organisations, policymakers and community stakeholders, employers and end-user organisations, young people, and the general public.

[19] Canto-Farachala P., Lorenz, U., Franco, S., Brounéus, F., Norvoll, R. and Hummer, P. *YouCount. D.5.7 Continuous, updated DEC and stakeholder engagement plan, and report on DEC activities*. Zenodo. doi.10.5281/zenodo.4812107

4 FAIR Data

4.1 Making data findable, including provisions for metadata

At this stage in the project, the consortium has not yet aligned its data documentation practices but plans to do this by the end of 2021 (before data recording begins in the case studies).

Discoverability of the data will be made possible through

- The publication of data on open repositories, such as Zenodo, linked to Open Aire, which will be our main repository. In addition, other national repositories for the case partners and the SPOTTERON CS platform, and potentially OSF (for publications), will be used.
- The use of unique identifiers for each data set and open publications.
- The consistent naming and versioning of files.
- The creation of a data inventory to list all data sets.
- The creation of metadata for each data set.

Data sets will thus be assigned a digital object identifier (DOI) in order to facilitate discoverability and identification. All the authors of the deliverables and the partners will register for an Open Researcher and Contributor ID (ORCID) if they do not have one already and will provide a link to this.

The actual choice of a metadata standard and naming convention system has yet to be finalised. The Data Documentation Initiative (DDI) appears to be the most relevant metadata standard.[20] The DDI is a widely used international standard for describing data in the social, behavioural, and economic sciences.

A file naming convention will be utilised to make the files more easily findable, accessible, and reusable. The files will be given names that provide a preview of the content, can be organised in a logical way (by date yyyy-mm-dd), contain a version name (e.g. Zenodo), and identify the responsible consortium member and author of the document. We will consider the use of Stanford guidelines to secure guidelines and procedures for file naming across consortium partners, particularly for qualitative data.[21]

The project will also provide key words to optimise possibilities for reuse. A systematic catalogue for related terms will be developed at a later stage to secure consistency in use among the

[20] Welcome to the Data Documentation Initiative | Data Documentation Initiative (ddialliance.org)
[21] Best practices for file naming | Stanford Libraries

consortium partners. At this stage, some important key words identified for the data packages include the following:

Data package 1: Citizen social science, youth citizen social science, community of open citizen social science, stakeholder mobilisation

Data package 2 & 3: citizen social science, youth citizen social science, social inclusion, youth, participatory action research, social innovation, policymaking, community, community development, refugees, disadvantaged youth, migration, disability

Data package 4: citizen science, citizen social science, youth, social inclusion, internet communication technology (ICT) platform, methods, open science, open data

Data package 5: citizen social science, youth citizen social science, social inclusion, social innovation, policymaking, community development, living labs, disadvantaged areas, transformative social science

Data package 6: citizen social science, youth citizen social science, evaluation, outcomes, process, costs and benefits, co-evaluation, SDG, MoRRi, impact

Data package 7: citizen social science, youth citizen social science, evaluation, costs and benefits of citizen science, impact, SDG, MoRRI, YouCount

4.2 Making data openly accessible

As set out in the EC-GA/Document of Action (DoA) (Section 2.2) and outlined in the project CA and PEH (D. 6.1), the YouCount consortium encourages the dissemination and publication of project results as soon as possible, albeit not before a decision has been made concerning the possible need for protection.

4.2.1 Which data will be made (openly) available?

As part of the OSc profile of the YouCount project, the data management in the project will aim to improve and maximise free access to and reuse of open research data generated by the project, while taking into account the need to balance openness and protect scientific and personal information according to privacy concerns (GDPR) and IPR, security, as well as data management and preservation questions (EU, Guidelines on FAIR Data Management in Horizon 2020, p. 3).

The need for confidentiality or limited access to data due to privacy concerns or commercial interests is outlined in the consortium CA and in the D6.3 IPR Plan.[22] Personal data access will be limited to authorised staff only, and only within the spatial and temporal limits negotiated with the data owners, and in no case beyond what is prescribed by the current legislation.

However, in general, the consortium partners will seek to collect and process the data in such a way that it can be made open at an early stage. Samples of open (quality assured) data from all sub-studies will be made open on the project webpage and open data repositories throughout the project period (e.g., D2.2 and D4.2 by April and June 2022). Directly or indirectly personal data will be treated as confidential according to WIC.

Open data will be made available for third parties to access and use for free in the YouCount app and by attaching a Creative Commons Attribution Licence (CC BY) to the data deposited (e.g., in Zenodo). Otherwise, we will waive all interests associated with copyright and database protection using the Creative Commons Zero (CC0) tool (see also, D6.3 IPR Plan).

For all user-generated content in the YouCount app (e.g., photos), the CC0 license will be applied. This will ensure interoperability of unique creative works without author attribution, which is in line with the 'right to be forgotten' of the GDPR, so the data and supplementary user-generated content can still be used even without the display of personal data as authorship.

We will also provide information via the chosen repository about the tools available to validate the results, e.g., specialised software or software code, algorithms, and analysis protocols. Where possible, these tools or instruments will be provided.

4.2.2 What methods and software tools will be needed to access the data?

Research data will be published in standard formats, such as DOCX, PDF, CSV, XLS, SPW and SAV, SQLITE, and data files (.dat), input files (.inp), and output files (.out) (Mplus), meaning that any standard software will be able to access the data, including open-source software.

Exports from user participation in the YouCount app will be stored as CSV files on the computers of administrator users of the project. Data from the platform (CSV) and samples of text excerpts can thus be categorised, coded, and analysed by content analysis of text, Excel, or SPSS software, or using qualitative software programmes, such as MaxQDA, ATLAS.ti, or NVivo.

[22] Norvoll, R. and Nedberg, H. (2021). *D.6.3 IPR plan*. Zenodo. doi.10.5281/zenodo.4720474.

4.2.3 How will access to data be provided in case of restrictions?

We do not currently anticipate having to deal with restricted access to data sets apart from those considered confidential (personal data) or IPR protected for commercial reasons, as described above.

Nevertheless, a public data inventory will be created with the publication status and an explanation if the data was kept private, allowing re-users to contact the data controller to ask about unpublished data sets.

Access to confidential data will be provided through username/password and in some cases, multifactor authentication (MS Teams or TSD).

Given the open nature of the data that will be generated in the YouCount project, we do not find a need for a specific data access committee. Assessments of access to data can be executed by the responsible researcher, DMP group, YouCount app Administration Group, or in line with the governmental bodies of the project, as outlined in the CA and PEH.

4.2.4 Intellectual property rights

An IPR plan has been developed for the project (D6.3, submitted April 2021). This plan will be updated throughout the project period.

4.3 Making data interoperable

4.3.1 How will the interoperability of data be assessed?

As described above, most of the data will be published in standard formats or in terms of open access. Data from the YouCount app will be available in a table format (CSV) and may be released as open data after being manually checked by the consortium for exchange and further use by researchers, institutions, organisations, and so forth. If released as processed open data, anonymisation procedures must be applied in accordance with the SPOTTERON terms of service/partner agreement (https://www.spotteron.net/partner-agreement).

Illustrative photos and recordings from R-YCs and LL activities can only be used according to the WIC.

In line with CoAct,[23] we will consider the use of the frictionless data standard developed by the Open Knowledge Foundation to publish data sets that can be exported in a tabular format (such as CSV). The frictionless data standard (https://specs.frictionlessdata.io/) is designed to maximise interoperability for data produced by research projects. These specifications provide a standard vocabulary of patterns for describing data sets, files, and tables.

4.3.2 What standard vocabulary will be used for all data types to allow interdisciplinary interoperability?

The consortium members are still in the process of defining the types of data collection methods and data that they expect to generate in the sub-studies and data packages, as described above. From these discussions, a standard vocabulary will emerge to be used across the research activities, which will align as much as possible with commonly used social science vocabularies.

4.4 Increasing data reuse (through clarifying licences)

4.4.1 How data will be licensed to permit the widest reuse possible?

As elaborated above, to ensure compliance with GDPR regulations, all personal data will be anonymised. We aim to publish the open data sets under a Creative Commons Public Domain Dedication (CC0), in accordance with the Open Aire guidelines.[24]

4.4.2 When will data be made available for reuse?

In addition to the samples of open data that will be made available in April and June 2022, all the publishable research data will be made available as soon as possible and before the end of the project (January 2024).

[23] Lombion, Cédric (2020). CoActD1.2: Data Management Plan. Zenodo. http://doi.org/10.5281/zenodo.4498287
[24] https://www.openaire.eu/research-data-how-to-license/

4.4.3 Will the project data be usable by third parties, particularly after the project ends?

The CC0 license that we intend to use allows for any kind of reuse of the data without restriction.

Open data will be available on the YouCount app and project webpage for reuse during the project period, as long as the home page is operative.

Anonymised data sets in the institutional repositories (partners) will be available upon request to anyone, as long as the repository owner legally exists.

4.4.4 What are the data quality assurance processes?

The data quality assurance processes are still under development, but will aim to control and document the consistency and quality of data collection according to scientific standards using data validation, peer data review, and systematic vocabularies.[25]

Currently, data quality will be ensured through different measures:

- Before the launch of data collection activities, the Executive Board (EB) and DMP group (if necessary) will consult with each partner to help them review their planned data structures, types, ontologies, and so forth according to the shared framework for data collection cross cases developed in WP 1–4.
- Before the publication of the qualitative data, data recording will be done in accordance with the developed data collection protocols and reviewed by the internal scientific reviewer (see D6.1 PEH). Transcription of interviews will follow guidelines for correct transcription (e.g., OsloMet/AFI). Open data or summaries of data (i.e., case reports) will be checked for proper anonymisation of data based on the guidelines developed by the Data Protection Authority/Zenodo and for adherence to correct metadata and naming.[26]
- The publication of the quantitative data set will follow the same basic procedures for quality checks (internal scientific review procedures and check of metadata and naming). In addition, the partners will validate their tabular data and ensure that their data exactly matches their expectations by potentially using the Frictionless Data's Good Tables pipeline or similar validation tools.[27]
- Deliverables, publications, and dissemination material will be subject to both ethical and security/confidentiality examination, according to GDPR Article 5(d).

[25] Cf. Science Europe: se_rdm_best_practices.pdf (scienceeurope.org)
[26] The anonymisation of personal data | Datatilsynet
[27] https://frictionlessdata.io/tooling/goodtables/

5 Allocation of Resources

5.1 What are the costs of making data FAIR?

The costs for developing and publishing the internet list are included in the EC-GA for the project and eligible if compliant with the grant agreement's conditions. No cost is presently foreseen, as Zenodo is a zero-cost long-term service. The cost of storing data on the SPOTTERON platform is included in the budget. No extra costs for data storage are foreseen.

5.2 Who will be responsible for data management?

The project coordinator (OsloMet) has the overall responsibility for proper data management in the project. OsloMet and consortium partners will, as elaborated on in D7.1 POPD Requirement No. 2, ensure that appropriate technical and organisational measures for proper processing and protection of the rights of the data subject are in place.

OsloMet will, in accordance with GDPR Article 30, keep records of processing activities through Meldearkivet (i.e., 'the Notification Archive') as part of their agreement with the NSD and the research database at OsloMet that includes all relevant information concerning the project.[28]

After discussions in the GA/EB and with the local data protection officials at OsloMet and the NSD, we find that the use of TSD at the University of Oslo is not required for all partners. All case partner institutions will thus have a shared responsibility as data controllers for their local cases with respect to data collection, processing, secure storage/transfer, and records, and to ensure that data management is conducted in accordance with legal and ethics requirements. SPOTTERON will only (apart from its responsibility for the CS platform as an SME) have the role of data processor in the project (Article 28) (see Terms of Use[29]).

A joint data controller agreement with all case partners and a data processor agreement with SPOTTERON will be signed in early autumn 2021. The agreements will duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and be made available to the participants through the use of written and oral informed consent.

[28] Forskningsdatabasen - Home (sharepoint.com)
[29] Terms of Use - SPOTTERON Citizen Science

Moreover, each WP leader will be responsible for their data management. Inside each WP, the responsible task leader will be co-responsible for the data collected in the task.

In addition, the DMP group, consisting of one representative from each partner (see Table 4), will serve as the responsible contact persons for the case and in collaboration with the project coordinator. As for the YouCount app, we have established an Administration Group that will be responsible for managing the data provided by SPOTTERON at each partner institution. SH will also act as the data-responsible partner on behalf of VA. The YouCount app Administration Group will have access to the exported CSV files in order to

- Delete and change content on the app.
- Send push messages to the apps and the community.
- Create events on the map.
- Administer comments (open question: how to handle different languages?).
- Administer contributions (= spots).

In addition, a number of researchers and R-YCS from each case partner will also be given the role of data moderators, where they will check the content provided on the app on a daily basis (see risk management below). These moderators will have skills in the national and additional languages (e.g., Arabic), as described above.

Table 6. Overview Data of the Administration Group of Consortium Partners

Partner	Name
OsloMet	Reidun Norvoll
VA	See SH (contact person VA: Fredrik Brounéus)
SH	Ann Mutvei Berrez
UCLan	Julie Ridley
FD	Susana Franco
UNIVIE	Isabelle Freiling
KTU	Giedrius Zvaliauskas
AAU	Michael Søgaard Jørgensen & Cathrine Marie Skovbo Winther
ESSRG	Alex Czeglédi
UNINA	Fortuna Procentese
SPOTTERON	Philipp Hummer

5.3 How long will data remain reusable?

The CC0 license that we intend to use for published data will allow for any kind of reuse of the data without restriction. See section 4.3.3 for more.

6 Data Security

6.1 What provisions are in place for data security?

In accordance with GDPR Article 5(f) and Article 32, the project will preserve the integrity and confidentiality of the participants by taking the necessary measures to prevent accidental loss/destruction of data, establish provisions to secure data storage, and protect personal data against unauthorised or unlawful processing. Data loss or breach of confidentiality will be notified according to law. Costs of data curation and preservation in high-security data storage systems at the participating universities are included in the budget.

In order to avoid loss of data, institutional servers will have automatic back-up solutions and regular maintenance of equipment. Back-up solutions will be used during data collection to prevent loss of data (e.g., two audio recorders or note taking) (see Table 7).

One aspect of data security is to ensure that data is safely stored in certified repositories for long-term preservation and curation. The choice of storage will be determined by data type; that is, raw data (most personal) or processed data, as described above. Storage of data can be distinguished by different types of storage:

- Short-term storage: Intermediary devices used to collect data and transfer it to longer-term storage before deletion (e.g., audio recorders, cameras, laptops), what we call 'external data collection devices' (NSD).
- Long-term storage: The servers where the data will be stored until its deletion. These can be university servers belonging to the institution, either as a PC with a common/shared area, PC local disk, or a cloud service with an appropriate security level due to institutional agreement.

Furthermore, storage devices can be grouped into personal and professional devices:

- Personal devices: These are the sole responsibility of the individual operating them and cannot be assumed to follow any kind of organisational policy (e.g., private PC/laptop, smartphones, tablets, cameras).
- Institution devices: These are professional devices operated by the researcher and managed by their affiliate organisations and are consequently operated and secured according to the guidelines of the relevant organisation (e.g., smartphones or audio recorders belonging to the institution).

E-mails can be accessed using either private or institutional e-mail accounts.

As detailed in Table 7, provisions for secure data processing and storage and choice of collection devices will depend on the level of confidentiality needed for the various data in all data packages.

In general, all partners will ensure that only PI/main researchers will have access to data and be able to share data with third parties, according to formal agreements and WIC.

As a basic rule, all confidential digital personal data (names, contact info), audio recordings of interviews, and unpublished photos, images, and videos will be stored on short-term external data collection devices (e.g., audio recorders) that belong to the institution, then transferred as soon as possible to the institution server belonging to the partner and stored on a secured area for long-term storage (and deleted on the external device). Some interviews might be recorded, summarised anonymously/pseudonymously by the researchers, and then deleted on the external device without being transferred to a PC.

WICs will be kept separate from the data and either be secured in a locked cupboard/archive at the partner institution or scanned and encrypted before being stored on the institution's internal system.

Nonsensitive data will be stored on the YouCount internal MS Teams platform owned by OsloMet. Only invited consortium partners and AB members who have signed a non-disclosure agreement will be invited as external guests and given access through password-protected individual e-mails. Some of the personal data (e.g., list of names and contact info) will be marked as confidential. The legal basis for this is informed consent (described in the WIC).

All partners will continuously evaluate the necessary level of secure data storage as the data collection evolves and take necessary measures. The use of short-term and long-term storage systems for each consortium partner is listed in Table 7.

Table 7. Short-Term and Long-Term Storage Systems for Each Partner Institution

Partner	Short-term storage/ External device	Long-term storage Institution (open, internal, and confidential data)	Storage sensitive data
OsloMet	Audio recorder, institution	Multifactor authentication OsloMet Teams on	TSD[30]

[30] Services for sensitive data (TSD) - University of Oslo (uio.no) TSD platform - Services for sensitive data which is part of the National Infrastructure for Managing and Storing Scientific Data in Norway: This is a platform for collecting, storing, analysing and sharing internally sensitive data in compliance with GDPR. More information about TSD is available on the following web-page: https://www.uio.no/english/services/it/research/sensitive-data/index.html.

	Smartphone, institution (photo/recording)	OneDrive/ Share Point, individual password-protected, private/confidential channels Open data platforms	
VA	Smartphones, tablets, and laptops	Data will be stored at SH	Data will be stored at SH
SH	Smartphones, tablets, and laptops	Data will be stored at the institutions MS OneDrive/Sharepoint in a specific YouCount-account, using two-step authentication.	Sensitive data will be stored at the institution´s MS OneDrive/Sharepoint in a specific YouCount-account with limited access using two-step authentication.
UCLan	Audio recorders, institution Surface pro (owned by UCLan) directly uploaded to secure OneDrive	Multifactor authentication UCLanData (university secure data storage system) UCLan Microsoft OneDrive/ Share Point, individual password-protected, limited access to shared storage for RTs only, password-protected Material data (e.g., drawings) stored in locked cabinet, locked office, PI, UCLan until digitised and uploaded to	UCLanData (university secure data storage system), only shared with appointed researchers

		OneDrive, at which point they will be destroyed using the university's system	
FD	Audio recorder/smartphone, institution Laptop, institution	Data will be stored at the institution's password-protected Google Drive	Data will be stored at the institution's password-protected Google Drive
UNIVIE	Audio recorder (institution) Institution, Laptop Paper notes (minutes) The data will be stored immediately upon conducting the data collections	Shared storage institution server UNIVIE, individual password-protected Open data platforms and OSc framework	See confidential data: Shared storage institution server at UNIVIE, individual password-protected Personal/sensitive data will not be made publicly available and will be removed as soon as possible
KTU	Audio recorder/smartphone Possibly notes on paper from workshops with YCS Institutional password-protected laptops for Zoom recordings	Institution PC, One Drive; the PI and identified RT members will have access to the folder; partners as well as national and institutional data protection officers and/or research ethics commission representatives will be provided access upon request	Sensitive data will be kept in a separate folder in One Drive and accessible to the PI and two authenticated RT members from KTU; access to the other partners' representatives will be granted upon request
AAU	Audio recorder (institution)	Institution PC, AAU official OneDrive data protected storage	Institution PC, OneDrive, password-protected, special secure area, only

		place, password-protected, only access researchers and on request (see above)	access researchers and on request (see above)
ESSRG	Audio recorder, not transferred PC (anonymised at once, summaries)	Institution PC, password-protected	Institution PC, password-protected
UNINA	Smartphone, private stored on cloud service (photo/recording) Laptop, institution	Institution server UNINA is individual password-protected	Confidential data: Shared storage institution server at UNINA, individual password-protected
SPOTTERON	ICT cloud and server infrastructure (currently AWS on European Servers) and in rotating encrypted backups on the server cloud	ICT cloud and server infrastructure (AWS, European Servers, encrypted backups)	Project-specific data dependant on the definition of the phase in drafting the app's contribution options for participants No sensitive research questions will be included but may come up (see risk management below)

Moreover, the SPOTTERON CS platform utilises several layers of security measures,[31] including

- SSL/TLS encryption of all transfers of personal data both in applications and on websites.
- Encrypted and secure access control to the administration interface for partners.
- Strong password-protected storage of access codes for administration tools and login areas.
- Server and cloud storage using respected and high-quality providers of such services.

[31] Terms of Use - SPOTTERON Citizen Science

Internal policies to avoid including third-party software or scripts (e.g., analytics, social media platform scripts, etc.) as much as possible will be applied.

In general, YouCount partners will anonymise all data as soon as possible during the research process and after the project ends for long-term storage and sharing on OSc platforms. Personal data (such as scrambling keys and important audio recordings) will be stored securely by some partners from 5 to 10 years after the project closure, as agreed with the national supervision authority. However, the data subject has the right to request the deletion of their personal data at any time.

6.2 Transfer of data

The choice of transfer procedures will follow the GDPR and the confidentiality level of the data. Please see Table 5 above for details concerning the transfer of data. These will mainly be textual data, tabular data, audio recordings, CVS files, and images.

At this stage, the YouCount project is primarily planning for the transfer of anonymous data (summarised case reports in English or statistical numbers) between partner countries that fall outside the GDPR. In addition, de-identified/anonymous data will be transferred from SPOTTERON to the Administration Group.

In each partner country, data will be transferred through short-term devices for secure long-term storage, as outlined in Table 7. Personal data in terms of CIS and WIC can be sent and received through institutional e-mail accounts. Audio files from interviews will be processed in a secure way, following the guidelines developed by AFI/OsloMet and translated and distributed to all partners. Confidential files will be transferred as ZIP files. WICs will be encrypted if digitally stored.

As for SPOTTERON, all data transferred over the internet will be encrypted via the Transfer Layer Security (TLS/SSL) protocol for all sensitive data exchanged between the servers and smartphone apps, interactive maps, and the project website (see also https://www.spotteron.net/citizen-science-app-features/privacy-data-safety). The transfer of data exports to the Administration Group is also encrypted via TLS/SSL.

6.3 Assessment of value and risk

The risk assessment of the project is outlined in the GA-DoA, and ethics challenges and risks will be elaborated on in D7.1 POPD Requirement No. 2, as will other deliverables concerning ethics. This DMP focuses on the value and risk regarding data management and protection.

A risk assessment of data in the project will include the three following activities[32]:

1. Identifying undesirable incidents (risk elements)
2. Assessing the risk—the likelihood combined with the consequences—of each identified undesirable incident
3. Evaluating and managing the risk by, for example, introducing measures that limit the risk

The assessment will build on the key values of protecting the rights and freedom of the participants and ensuring that the data processing is lawful, fair, and transparent and directed to maintain participants' personal integrity and dignity. Potential threats to these values are a lack of real participation/co-determinism and a lack of transparency or predictability concerning the collection, use, and procession of personal data.

Subsequently, the risk assessments concerning data management will take three factors related to data protection into consideration: confidentiality, integrity, and accessibility. The risk assessments will be based on threats that may arise in connection to the collection of raw data, handling of the scrambling key, and the research file. Threats can be both people and systems, and often a combination of the two. Subsequently, a risk element is a violation of CIA (C = Confidentiality, I = Integrity, A = Availability; see definitions provided below) and can be split into levels of low risk (green), 2–3 ; medium risk (yellow), 4–5; and high risk (red), 6–8.

- Confidentiality: Ensure that information does not become known to third parties
- Integrity: Ensure that information is not inadvertently changed by third parties
- Availability: Ensure that information is accessible as needed
- Vulnerability: An inherent weakness in a system, person, or building that can be exploited by a threat.

The overall risk assessments concerning data management in the YouCount project are, at this stage, considered low or medium given the limited level of personal data and the low level of intruding activities during the project period. Potential risks identified at this stage are reidentification or pseudonymous data (due to small samples), loss of confidential data, and lack

[32] Risikovurdering og verdivurdering | FoU-håndbok - Ansatt - minside (oslomet.no)

of ability for the youths to understand the consequences of participation in the research before supplying WIC or giving consent with enough or understandable information.

Given the targeted youth groups, there might also be a potential risk for participants to be exposed to discriminating and negative responses when partaking in dialogue forums or LLs or when providing data in the app (See also, D7.1 POPD Requirement No. 2). Some disadvantaged groups (e.g., migrants/refugees) might also be anxious concerning anonymisation or use of data in collaboration with public authorities (e.g., in LLs or national workshops) due to a lack of trust or being in vulnerable social situations. The consortium is also well aware of the research challenges (e.g., low data quality and breach of confidentiality) involved with R-YCS conducting co-research as laypeople and will safeguard against this (see Ethics below).

6.4 Risk management

All potential risks related to the sub-studies will be continuously evaluated and mitigated throughout the project period in the consortium as a whole and in each case country according to the targeted participant groups (see also, Ethics).

The SEB and AB will provide support for security and risk assessments throughout the project period. YCS will also be included in risk assessments of data and the need for data protection in the development of data collection strategies/tools and data processing, as seen from youth's own perspectives.

The project coordinator at OsloMet will carry out a value and risk assessment according to the university procedures, and as soon as possible after the NSD has given its approval by filling out a template for risk assessment in research and a plan for risk management. This will be stored at the administrative and project levels and updated throughout the project period.[33]

The project partners will then implement several measures for each undesirable incident involving a risk factor that exceeds the institution's acceptable risk level. This will include implementing measures that reduce the likelihood or consequences of an incident and strategies for overcoming challenges along the way, including the following safeguard measures:

- Data minimisation
- WIC for all participants

[33] https://ansatt.oslomet.no/en/assessment-value-risk?p_l_back_url=%2Fen%2Fsok%3Fq%3DROS%26oterm%3Dinfo

- Data controller/procession agreements with all partners, including secure data storage/procession, confidentiality, authorised access, and risk mitigation
- Regular updating of the DMP, including risk assessments and measures required in collaboration with the DMP and Administration Group for the YouCount app
- YouCount app:
    - Discussions with YCS about proper use of the app
    - User manual for the YCS, including terms of use, informed consent procedures, and advice on how to use the app appropriately (dos and don'ts)
    - Regular control of the posts uploaded on the YouCount app by administrators/moderators in each case country
    - Information for users on the possibility of reporting unwanted content and responses on the app as well as blocking other users
    - The reporting will be checked by the administrators/moderators
    - Interactive inputs experienced as harming/violations will, according to the actual content, be discussed with the YCS (if known), or the user will be excluded from the app

7 Ethical Aspects

Ethical aspects are of utmost importance for the YouCount project and are included as part of the RRI framework, the project objectives and outputs, the organisation of the project (such as the SEB), and the tasks and deliverables focusing on excellence in ethics (e.g., WP1 Framework Development). Ethical challenges and solutions to these are described in the ethics chapters/sections in the DoA, Chapter 2, and will be further elaborated in the ethics deliverables (due July 2021) concerning recruitment and consent procedures and POPD 2 requirements, including how we will deal with vulnerable youth.

YouCount will adhere to the legal and ethical requirements concerning data collection, processing, and sharing, as described above. All partners must obtain informed consent from the subjects of their studies, and informed consent will also be included in the YouCount app and terms of use. The WICs will be based on the template provided by the NSD (see Appendix A, which includes the requirements and will be adapted to the local case and targeted youth group). The informed consent form includes a section on the collection and storage of personal data in databases, a statement regarding the period of data storage and possible use for future research, and contact information for the data controllers. Furthermore, participants will be informed that they or their legal representative may request that data be deleted when this data has not already been used in publications or presentations. To ensure 'real' informed consent, the WIC will be adjusted to age, language skills, and the targeted groups in each case country and on the YouCount app.

In addition, efforts will be made to secure voluntariness throughout the whole research process and to underline the possibility of withdrawing consent to participate at all stages without negative implications, since this might be particularly important for young people and disadvantaged groups of youths. All case partners will also provide oral information to the youths and stakeholders at the local level throughout the project period as needed.

In addition to WIC, all R-YCS will be interviewed by the researchers before finalising their participation to ensure the appropriateness of their roles as R-YCS and to inform them about the project and the implications of participation. The interview will also include questions regarding the suitable level of participation (number of hours, tasks, and time period) and appropriate rewards to safeguard tailored participation and avoid experiences of exploitation. This will be an ongoing conversation.

To ensure good ethics conduct, voluntariness, confidentiality, and informed consent, the R-YCS will undergo training courses before beginning their research and innovation activities. This might be important since the R-YCS will have an active role in the recruitment of other YCS and work in some of the same areas where they might know the youths from before. It is therefore important to ensure that C-YCS are well aware of the principle of voluntariness and their ability to reject participation or withdraw consent at any time. All R-YCS will be supervised and guided by

researchers throughout the project period. In addition, the project will include peer support in terms of working together in groups, such as the Youth AB, online meetings, and participation in the consortium meetings.

The need for parental/guardian consent and how this should be obtained in the best way will be assessed together with the NSD and national supervision authorities when the data collection methods are more developed. How parental/guardian consent should be integrated into the YouCount app will be considered together with consortium partners, the NSD, and SPOTTERON in autumn 2021.

8 Other Issues

OsloMet, as the coordinator and data controller, will submit an obligatory notification form to the NSD, Department of Data Protection Services, for research projects involving personal data to ensure legal access to the necessary personal data for research.[34] The need for a Data Protection Impact Assessment (DPIA) will be assessed by the NSD, as elaborated on in D7.1 POPD Requirement No. 2. In addition, data protection and ethical aspects will be assessed by the local data protection officials at OsloMet to ensure that personal information is processed securely and for limited purposes only at the institutional level.[35]

Furthermore, as elaborated in the ethics deliverables, the consortium will ensure continuing compliance and will consider relevant revisions to the mentioned legislation and directives. Each partner will be held responsible for the fulfilment of all legal and ethical requirements in their respective countries. If warranted by national legislation, protocols that are used in the network will need to be submitted to and approved by local ethical review committees. All WP leaders will need to deliver approval for the project coordinator to enable adequate registration and monitoring. If requested by institutional ethical review committees or national authorities, access may be given to records related to the programme, as stated by national law.

[34] About NSD - Norwegian Centre for Research Data | NSD

[35] Personvernombud for administrative behandlinger | Helse, miljø og sikkerhet - Ansatt - minside (oslomet.no) https://ansatt.oslomet.no/en/research-ethics

9 Appendixes

Table 8: Appendixes

Appendix A NSD Template Informed consent

This is a template for informed consent when processing personal data in research projects. It can be used for surveys, observation, interviews, sound recordings, etc.

Please delete the text in italics and insert your own text

NB! Information must be concise and easily understandable for the reader.

Use clear and simple language, headings and bullet points, active (not passive) language, avoid foreign words.

Are you interested in taking part in the research project "(insert title of project)"?

This is an inquiry about participation in a research project where the main purpose is to *[Insert brief description of the project purpose]*. In this letter we will give you information about the purpose of the project and what your participation will involve.

Purpose of the project
Describe the purpose of the project in more detail and indicate the scope of the project.
Briefly outline the project's objectives / research questions
Indicate whether it is a research project, a doctoral thesis, a bachelor's/master's thesis, other student project etc.

If you or others will use the collected personal data for other purposes (e.g. teaching or other research projects), describe these other purposes.

Who is responsible for the research project?
[Insert name of the institution(s)] is the institution responsible for the project.

If applicable, provide names and describe cooperation with other institutions, external entities etc.

Why are you being asked to participate?
Describe how the sample has been selected (population, selection criteria and how many people have been asked to participate), so that it is clear why the person is receiving this inquiry

If applicable, indicate whether you have received the person's contact details from another (and indicate any approval/permission obtained in order to do this), or whether another has sent out this information letter on your behalf.

What does participation involve for you?
Describe the methods (online/paper-based survey, interview, observation, etc.), the scope, what type of information will be collected and how the information will be recorded (electronically, on paper, sound/video recording), e.g.:
« If you chose to take part in the project, this will involve that you fill in an online survey. It will take approx. 45 minutes. The survey includes questions about (describe the most important questions/topics). Your answers will be recorded electronically»

If applicable, indicate that you also will collect information about the participant from other sources – such as registers, records/journals, educational records, other project participants, etc., e.g.:
«I will also ask your teacher to provide information about you in an interview. It will be information about (describe the most important questions/topics). I will record the interview and will take notes»

If children will participate, provide information that parents/guardians may on request see the survey/interview guide etc. in advance.

If there are multiple groups of participants, be clear about what participation will involve for each group, or give a separate information letter to each group.

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Expand on this if the person being asked to participate is in a situation where they are dependent on the person asking. E.g. «It will not affect your treatment at the hospital / your relationship with your school/teacher, place of work/employer etc.(..)»

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act).
Describe who, in connection with the institution responsible for the project, will have access to the personal data (e.g. the project group, student and supervisor, etc.)
Describe which measures you will take to ensure that no unauthorised persons are able to access the personal data, e.g. «I will replace your name and contact details with a code. The list of names, contact details and respective codes will be stored separately from the rest of the collected data», you will store the data on a research server, locked away/encrypted, etc.

If applicable, indicate:
the name of the data processor that will collect/work with/store data, e.g. online survey provider or transcription service
that persons from other institutions will be given access to the personal data, name the institutions, indicate the number of people and what type of information they will have access to (e.g. whether they will have access to data that can be directly linked to individual participants, or to collected data that has been de-identified)
that personal data will be processed outside the EU (e.g. fieldwork, analysis, cloud computing, conferences), name the institution and country, describe security measures.

Describe whether participants will be recognisable in publications or not, and to what extent. If applicable, indicate what type of personal information will be published (e.g. name, age, occupation etc.).

What will happen to your personal data at the end of the research project?
The project is scheduled to end *[insert date]*. *Describe what will happen to the personal data, including any digital recordings, at the end of the project.*

If the collected data will not be anonymised at the end of the project: indicate the purpose of further storage/use of personal data (e.g. verification, follow-up studies, archiving for future research), indicate where the personal data will be stored, who will have access to it, and the date for anonymisation (or, if applicable, specify that the personal data will be stored indefinitely and give a reason for this).

Your rights
So long as you can be identified in the collected data, you have the right to:
access the personal data that is being processed about you
request that your personal data is deleted
request that incorrect personal data about you is corrected/rectified
receive a copy of your personal data (data portability), and
send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with *[insert name of institution responsible for the project]*, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with data protection legislation.

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:
[Insert name of institution responsible for the project] via *[insert name of the project leader]*. *For student projects you must include contact details for the supervisor/the person responsible for the project, not just the student.*
Our Data Protection Officer: *[insert name of the data protection officer at the institution responsible for the project]*

NSD – The Norwegian Centre for Research Data AS, by email: (personverntjenester@nsd.no) or by telephone: +47 55 58 21 17.

Yours sincerely,

Project Leader (Researcher/supervisor)

Student (if applicable)

Consent form

Consent can be given in writing (including electronically) or orally. NB! You must be able to document/demonstrate that you have given information and gained consent from project participants i.e. from the people whose personal data you will be processing (data subjects). As a rule, we recommend written information and written consent.
For written consent on paper you can use this template
For written consent which is collected electronically, you must choose a procedure that will allow you to demonstrate that you have gained explicit consent (read more on our website)
If the context dictates that you should give oral information and gain oral consent (e.g. for research in oral cultures or with people who are illiterate) we recommend that you make a sound recording of the information and consent.

If a parent/guardian will give consent on behalf of their child or someone without the capacity to consent, you must adjust this information accordingly. Remember that the name of the participant must be included.

Adjust the checkboxes in accordance with participation in your project. It is possible to use bullet points instead of checkboxes. However, if you intend to process special categories of personal data (sensitive personal data) and/or one of the last four points in the list below is applicable to your project, we recommend that you use checkboxes. This because of the requirement of explicit consent.

I have received and understood information about the project *[insert project title]* and have been given the opportunity to ask questions. I give consent:

to participate in *(insert method, e.g. an interview)*
to participate in *(insert other methods, e.g. an online survey) – if applicable*
for my/my child's teacher to give information about me/my child to this project (include the type of information)– if applicable
for my personal data to be processed outside the EU – if applicable
for information about me/myself to be published in a way that I can be recognised (describe in more detail)– if applicable
for my personal data to be stored after the end of the project for (insert purpose of storage e.g. follow-up studies) – if applicable

I give consent for my personal data to be processed until the end date of the project, approx. *[insert date]*

(Signed by participant, date)

YouCount

Youth Citizen Science

PARTNERS: