BUDGET IT

Building Gender+ Equality Through Gender+ Budgeting For Institutional Transformation

Data Management Plan

Grant Agreement № 1010904391

Project Start Date	01.01.2023
Duration of the project	36 Months
Work Package	WS
Deliverable Number	D.5.1
Deliverable Leader	Branko Radulović
Submission Date	30.06.2023
Authors	Branko Radulović, Lidija Živković
Institution	University of Belgrade, Faculty of Law
Email	bradulovic@ius.bg.ac.rs

Modification Control

Version	Date	Description and Comments	Author
0.1	01.04.2023	First Draft	Branko Radulović
0.2	05.06.2023	Second Draft	Lidija Živković
0.3	30.06.2023	Last version	Branko Radulović

List of Contributors

Suzana Ignjatović

This project has received funding from the European Union's Horizon 2023 research and innovation programme under grant agreement N° 1010904391.

Table of Contents

Introduction

The BUDGET-IT Project aims to advance inclusive gender+ equality in the institutions of the widening countries (Bosnia, Serbia, and Turkey) by implementing gender+ budgeting as a tool of institutional transformation. The BUDGET-IT Project will collect data from institutional sources (universities and municipalities) and human subjects (focus groups and surveys). Baseline data will be processed and analyzed as part of gender+ equality plan (re)evaluation. Human subjects are also involved in the interventions and activities related to institutional transformation.

The BUDGET-IT Data Management Plan (DMP) is a document that outlines how research data will be collected, organised, stored, preserved, shared, and reused throughout the research project and after its completion. It is a tool that helps researchers manage their data effectively and efficiently, ensuring that the data is well-documented, secure, and accessible to others who may want to use it- Additionally, the DMP will put down the procedure for data collection, consent procedure, storage, protection, retention and destruction of data, and confirmation that they comply with national and EU legislation.

DMP will be revised and updated during the project lifecycle.

The DMP will also link these activities to the BUDGET-IT partners and underline their responsibilities with respect to all aspects of data handling.

DMP covers:

- Objectives
- H2020 Principle
- BUDGET-IT DMP policy
- Data handling during and after the project
- What types and formats of data will be generated/collected?
- Whether the data be shared or made open-access, and how?
- How data will be curated and preserved
- Ethics

The DMP is intended to be a living document which will be adjusted to the specific needs during the lifecycle of the project, and will be updated and adapted each year of the project as needed.

Project Background and Objectives

The Deliverable describes the approach and plans that have been agreed within Work package 6 to promote and assist BUDGET-IT partners to achieve their local regulatory compliance for GDPR and to help the Consortium represent best practice for meeting these requirements. Successful compliance with GDPR relies on the ability for individual partners to understand their requisite data flows as well as agree with other partners the manner of data provision, receipt, and subsequent obligations.

For a collaboration across multiple partners within different regulatory jurisdictions, a single statement as to compliance and plan to ensure it across all partners is neither possible or appropriate. Hence, besides DMP, partners are strongly advised to consult:

https://ec.europa.eu/assets/rtd/ethics-data-protection-decision-tree/index.html

DMP has following objectives:

- To guarantee the appropriate and safe management of data collected;
- To make all the partners aware of the data protection process;
- To ensure compliance with the 'ethics requirements' set out and
- To ensure that all activities conducted under Budget-It adhere to the highest ethical standards.

The DMP will be utilized as input in the following project tasks:

- WP2 – (Re)Evaluating GEPs: Task 2.1 Data collection; Task 2.3 Gender Equality Audit and Monitoring (GEAM) Survey; Task 2.4 Training for inclusive GEPs for universities and municipalities;
- WP3 – Implementation of Gender+ Audit and Gender+ Budgeting: Task.3.1 Gender+ budgets; Task 3.2 Integrated GEP-GB for all partners and audit guideline.
- WP5 – Data Management and Ethics: Task 5.1 (Data Management Plan); Task 5.2 (Data Management Workshop); Task 5.3. (Ethics); WP6 (Ethics Requirements).

1. Data Management Plan (DMP) in the Context of Horizon Europe

1.1Open Resource Data Pilot

A recent development in Horizon 2020 is the Open Research Data Pilot, which aims to improve and maximize access to the research data generated by EU-funded projects. The EC provided a document with guidelines for project participants in the pilot.

The guidelines address aspects like research data quality, sharing, and security. According to the guidelines, project participants will need to develop a DMP. This document has been produced following these guidelines and aims to provide a consolidated plan for BUDGET-IT partners in the data management plan policy that the project will follow. This document is the first version delivered in D5.1 of the project.

Benefits of taking an active approach to research data management include increased speed and ease of access, efficiency (fund once, reuse many times), and improved quality and transparency of research.

In Horizon 2020, the Commission committed itself to running a flexible pilot on open research data (ORD Pilot). The ORD pilot aims to improve and maximize access to and re-use of research data generated by Horizon 2020 projects. It considers the need to balance openness and protection of scientific information, commercialization and IPR, privacy concerns, security as well as data management and preservation questions.

More information:

- https://data.europa.eu/euodp/en/data/dataset/open-research-data-the-uptake-of-the-pilot-in-the-first-calls-of-horizon-2020
- https://ec.europa.eu/info/research-and-innovation_en#view=fit&pagemode=none

1.2 FAIR Data

In general terms, research data should be 'FAIR', that is findable, accessible, interoperable and re-usable. These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution.
More information:

- https://www.force11.org/group/fairgroup/fairprinciples
- https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

2. BUDGET-IT Data Management Policy and Open Access

The BUDGET-IT Data Management Plan (DMP) will determine and explain which of the research data you generate will be made open – meaning free of charge online access for any user. The plan will include details on how make your research data findable, accessible, interoperable and reusable (FAIR).

2.1Data Management Plan

The DMP will be regularly updated and reported in a revised DMP in the continuous periodic reports. It will follow the FAIR guidance (data findable, accessible, interoperable and reusable). This plan will evolve during the lifetime of the project in order to present the status of the project's reflections on data management.

The project will generate data for the purpose of developing gender equality plans and gender budgeting. During the organization of these activities, the organization team will collect real people data to facilitate the project output.

- The BUDGET-IT Project will collect data from institutional sources (universities and municipalities) and human subjects (focus groups and surveys).
- Baseline data will be processed and analyzed as part of gender+ equality plan (re)evaluation.
- Primary data (the GEAM survey and focus groups) and secondary data (institutions) will be used for different activities during the project: intervention, dissemination, and exploitation.
- All personal data will be managed following the EU-GDPR principles of data minimization, storage limitation, integrity, and confidentiality.

Primary data (the GEAM survey and focus groups)

In focus groups, all personal information will be anonymized by pseudonymization in the transcripts and publications.

Other dissemination, communication, and exploitation methods (policy briefs, conference papers) must not lead to a breach of agreed confidentiality and anonymity.

Alternative identifiers will be used to prevent any unintended indirect identification.

Audio recordings will be deleted from recording devices after being transcribed.

The GEAM survey will be administered online, so the data needs to be protected from unauthorized access and misuse.

All personal data from the survey and focus groups will be available only to authorized persons.

The data will be stored with the highest level of security.

Protecting privacy and confidentiality of survey respondents is a key concern and has to be considered carefully before preparing and launching a survey. Before launching a survey,

administrators will be required to download and complete the following data protection declaration and confidentiality agreement.

ACT_GEAMPreLaunch_DataAgr_10SEP2021.pdf (act-on-gender.eu)

For the GEAM survey, privacy implies to give respondents relative control over data entry ("what" and "when"), including the possibility to opt out and delete their data at any moment during the submission process. Confidentiality implies that result data is anonymized and stored in a secure way to prevent unauthorized access.

Each Consortium member that administers a GEAM questionnaire will strictly follow requirements of The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 and will be responsible for content and handling of resultİNG data. Each Consortium member shall follow the GEAM Manual

ACT Gender Equality Audit and Monitoring (GEAM) (act-on-gender.eu)

The survey administrators will make sure that the GEAM survey is accompanied by adequate information for respondents to provide informed consent. Specifically, each survey administrator must provide:

- Information about your organization: including name and contact details, details of your representative (if relevant) and contact details of your Data Protection Officer.
- Information about the type of data you will collect for example, gender, contract details, salary, etc.
- The purpose of collecting the data: including what you will use it for and whether it will be used to make an automated decision; the legal basis for using the data including any 'legitimate interest' relied upon. -Who will receive or have access to the data: for example, members of an Equality, Diversity and Inclusion committee, Human Resources, or a Gender Equality Planning group.
- Other information: including whether the data will be transferred, stored, or processed outside the EU and on what basis; how long the data will be stored for; what security arrangements are in place to protect the data; whether provision of the data is required and the consequences of not doing so.
- Data subjects' rights: the right to be informed; right of access; right to rectification; right to erasure; right to restrict processing; right to data portability; right to object; and rights in relation to automated decision making and profile. Contact information: who they can contact in relation to questions or complaints

Questions and response options may need to be adapted according to an organization's or country's legal requirements where it affects monitoring practices, policies and the terms used to describe populations. Survey administrators, when editing questions and response options on protected characteristics, need to be aware of the rights and permissions in their country. For instance, they need to know if permissions to collect data on

protected characteristics such as sex, race and sexual orientation differ or require an organization to re-phrase the language in the survey to be in line with regulatory standards.

Draft Inform consent forms for surveys and focus groups are provided in the Ethics Plan. They provide comprehensive information about the study and their role in the study.

The GDPR draws a distinction between "personal data" and "personal sensitive data". Personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (article 4.1). Sensitive personal data or special categories of personal data refers to information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation (article 9).

The survey will include items inquiring about Sensitive Personal Information (e.g. sexual orientation, health impairments or reporting discrimination associated with ethnicity). However, the GEAM does not contain questions regarding direct personal identifiers such as social security number, names, email addresses or similar. Thus, the collected data is anonymous on a very basic level However, respondents might provide certain identifiers in open text questions such as organizational names or names of colleagues which unintentionally can identify their (and others) contributions.

To this end, each partner will consider whether the person to whom the data pertains might still be identified through indirect identifiers (e.g. occupation, salary); by people who know them or the context; or by those who have access to other information which, when combined with the data, might allow them to be identified. In these cases, it is necessary to take further action to anonymize the data.

The GDPR contains a strict definition of anonymity: it considers data anonymous only when it cannot be identified by any means "reasonably likely to be used either by the controller or by another person". This means that if the data could be re-identified by any person using 'reasonable effort', it would not be considered to be anonymized, and respondents would need to be made aware of this during the consent process described above. For example, if a report summarizing the proportions of men and women working in individual roles only included one female respondent from a specific university department, it is possible for this single individual to be identified by her colleagues.

Whenever there is a small number of respondents within a certain category, this identifier may need to be removed before sharing to prevent breaching participant confidentiality and anonymity. To this end consortium members will refrain from sharing the raw data and instead only share the results of the survey in summary tables that have small numbers represented as less than values (e.g. groups with fewer than 5 individuals are represented as '< 5' instead of listing the exact frequency) or by applying a rounding strategy.

2.2Open Access

Selected deliverables which have been classified as public documents will be available via the project's website.

BUDGET-IT will ensure immediate Open Access to peer-reviewed scientific publications and communications relating to project results in trusted repositories (such as Zenodo) no later than the publication date. All publications will be published under an open licence, ideally the Creative Commons Attribution licence (CC BY) or equivalent. When disseminating project results, Budget-It will look to publish in relevant journals which are in the top 20% of Open Access scientific journals in gender+, work and education.

The project will also aim for 'early and open sharing', as and where appropriate considering relevant exceptions (e.g., journal policies), through means such as pre-registration, registered reports and pre-prints.

3. Data Summary

Public documents within the consortium are processed and managed by the project coordinator. Other data generated throughout the project (report, data and others) are managed and stored by the team responsible for data generation.

The following table shows the data type, the origin of the data for the BUDGET-IT project. Mainly, personal data will be collected. Access to personal data will be restricted to necessary parties within the consortium.

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

Table 1: Data Summary

	Data type	**Origin**	**Data control responsibility**
1	Partner contacts and stakeholders list collection	Open Source Data	KHAS Project Management
2	Data from institutional sources (budgets, GEPs) and official statistics	Open Source Data	Content and handling will be responsibility of each survey administrators (partners)
3	GEAM Survey data results	Primary Data	Content and handling of result data will be responsibility of each survey administrators (partners)
4	Focus group data	Primary data	Content and handling of focus group data will be responsibility of each partner
5	Personal data of Participants-workshops training groups and materials	Primary data	UA/UBS/SSST/UBG

The following list highlights the type of data that will be produced, used and made openly available under the guise of the project:

- **Partner contacts collection and stakeholders list:** BUDGET-IT Project partner information and stakeholder list data (such as university contact, contact names and emails and pictures etc.) will be integrated in the public deliverables but only after consent has been secured.
- **Digital security solutions collection:** Data openly available

- **Online training groups data:** The data from online training groups (recordings, protocols and transcriptions) will only be published after obtaining consent from all participants.
- **Training program for inclusive GEPs data**: The data from training program for inclusive GEPs (recordings, protocols and transcriptions) will only be published after obtaining consent from all participants.

4. Data Security

For the project's duration, datasets will be stored on the responsible partner's storage system. Every partner is responsible for ensuring that the data are stored safely and securely and fully compliant with European Union data protection laws. After completing the project, all the responsibilities concerning data recovery and secure storage will go to the dataset repository.

To raise the awareness of GPDR and data security, the project has provided a Data protection, data management and GPDR workshop for the project partners on how to handle the data with Prof. Branko Radulović, the Data Protection Officer for the project.

Throughout the project, the management team and data protection officer will communicate with the necessary bodies to ensure protection data generated and collected under the project.

4.1Storage

Storage indicates the medium and location of the backups. It is the responsibility of the project partner who collects the data (to ensure that the data is regularly backed-up and stored securely for the lifetime of the project. Data should be stored protected by password or using an encrypted shared drive.

In either case, the folder in which the data are stored will be restricted. If you store it on an external (flash) drive, the drive should be encrypted or password protected in order to prevent unauthorized access in case of loss.

We distinguish the following types:

• **Network drives** - These are secure and backed-up regularly. Once in a month, air gapped offline backed up by the project management team. Access rights to these data is checked regularly. Access logs are also inspected once in a month. In case of any suspicion on unauthorized access to the data, the situation will be quickly reported to the data protection officer.
• **Local drives** – Data on PCs and laptops can be lost because of technical malfunction or the loss of the device itself. These are convenient for short-term storage and data processing but should only be relied upon for storing master copies when backed-up regularly. The owner of the PCs and laptops are responsible to install anti-virus systems to ensure utmost security as an end-user. If this equipment is given by their universities, the holder should obey the rules of its institutional IT. If any of the computers are compromised by a phishing or ransomware attack, the user is responsible to inform the data protection officer and the relevant IT management to protect the data or follow-up action. If the project partner is accessing the data with mobile devices, they must manually enter access information each time. If any project member loses any of their mobile devices which they have used to store or access the

data, they should immediately inform project management and the data protection officer to take necessary steps forward to prevent any leaks and to enable the change of access credentials.

• **Remote or cloud storage** – For the facilitation of the project, the project management will use Microsoft Products which claims its appropriateness to GDPR requirements. The data stored in cloud is minimized as asked by the regulation and access rights organized by the project management. When the relevant phase of the project ended, the project management and partners are responsible for downloading the data to an offline disk and deleting all files in the cloud. The members of the project will not keep redundant data in the cloud storage. Access codes for these files will be changed periodically by the data processor. In case of any risks or security infringement, the data processor will inform the necessary bodies and the project partner and the data protection office to make necessary steps to secure the data and data subjects.

• **External portable storage devices** (external hard drives, USB drives, Blue rays, DVDs and CDs) - As the project does not aim to keep datasets for long periods of time, we utilize rewritable external hard drives. Partners may obtain separate devices solely for project usage and they will be stored separately. This precaution is designed to limit the plugin time of device and the digital hygiene of the files inside it. To access the files, the device will be password protected and the password will be changed every three months.

• **Web site and social media:** A two-level authentication system will be used for BUDGET-IT social media accounts on Twitter, Instagram and Facebook. The passwords will be shared with only 2 other individuals in addition to the Coordinator and will be changed regularly to keep them secure and private. The passwords for the website will also be changed regularly and kept secure with a two-level authentication system.

4.2 Data access

The process of data collection will in many ways determine who has access to the data. Data security is needed to prevent unauthorized access otherwise data might be intentionally or unintentionally disclosed, changed or deleted. The storing partners are responsible for ensuring data security. The level of security required depends upon the nature of the data – personal or sensitive data need higher levels of security. All correspondence and documents related to the project will be backed up every month to an offline medium.

The access controller is responsible for the access management of the data. Access management is the description on how the access to the data will be managed. Data can be labelled as:

- Public information – Project Outputs
- Personal Data- No sharing

Access is limited to the appointed persons, functions and groups. It can be extended on demand. The access to the data of the study will be managed by the assigned access controller for each data type. It will be done according to the access management description linked with the data type.

All data files will be transferred via secure connections and in encrypted and password-protected form (for example, with the open source 7-zip tool providing full AES-256 encryption: http://www.7-zip.org/ or the encryption options implemented in MS Windows or MS Excel). Passwords will not be exchanged via e-mail but in personal communication between the partners.

5. Ethical Aspects

Data protection and good research ethics are major issues for the consortium of this project. Good research ethics demand great care and require the prevention any situation where sensitive information could be misused. This is what the consortium wants to guarantee for this project.

All processes of data generation and data sharing must be documented and approved by the consortium to guarantee the highest standards of data protection. BUDGET-IT partners must comply with the ethical principles as set out in Article 14 of the Grant Agreement and Annex 5, which states that all activities must be carried out in compliance with:

- Ethical principles (including the highest standards of research integrity as set out, for instance, in the European Code of Conduct for Research Integrity and including avoiding fabrication, falsification, plagiarism, or other research misconduct).
- Applicable international, EU, and national law (in particular, EU Directive 95/46/EC).

The BUDGET-IT consortium confirms that each partner will check with their national legislation/practice and their local ethics committee. That will provide further guidelines on data protection and privacy issues, in terms of data protection.

Any procedures for electronic data protection and privacy will conform to Directive (EU) 2016/680 and Regulation (EU) 2016/679 (GDPR) on the protection of personal data and its enactments in the national legislations. The process of adhering to the applicable regulations begins with a thorough investigation of the EU and National research projects' ethical guidelines as well as the examination of the directives regarding privacy and protection of personal data and free movement of data issues.

- Information gathered from the participants should be kept confidential, unless specific consent to be cited is given by the participant.
- Information gathered should be anonymized and used only for the purpose for which it was collected.

In case the collected data contains personal information, data protection principles and legal requirements extracted from Regulation 2016/679 and national laws will be taken into consideration.