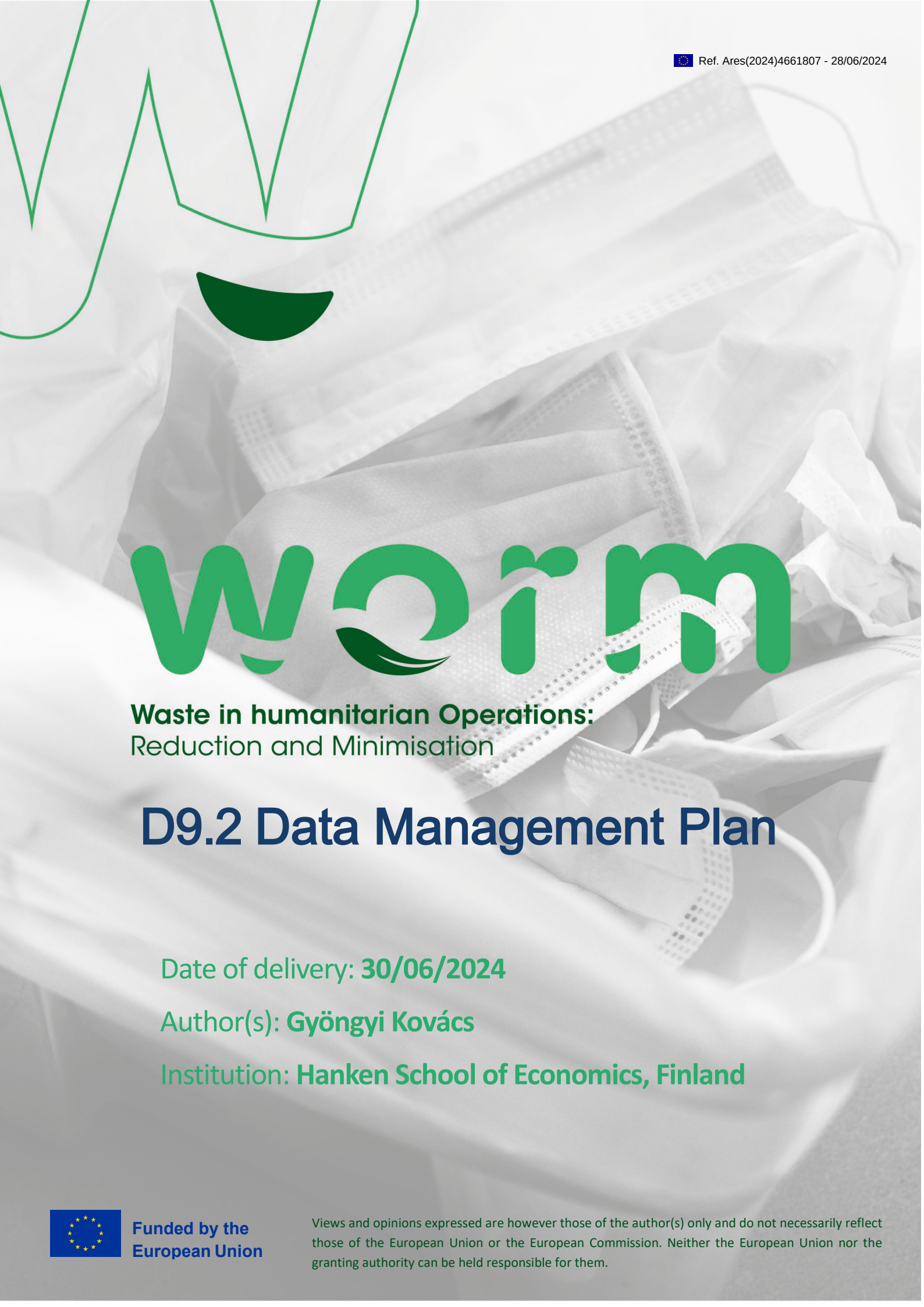

WORM

Waste in humanitarian Operations:
Reduction and Minimisation

D9.2 Data Management Plan

Date of delivery: **30/06/2024**

Author(s): **Gyöngyi Kovács**

Institution: **Hanken School of Economics, Finland**

Funded by the European Union

DOCUMENT TRACK INFORMATION

PROJECT INFORMATION	
Project acronym	WORM
Project title	Waste in humanitarian Operations: Reduction and Minimisation
Starting date	01/01/2024
Duration	24 months
Call identifier	HORIZON-CL6-2023-CIRCBIO-01
Grant Agreement No	101135392

DELIVERABLE INFORMATION	
Deliverable number	D9.2
Work Package number	WP9
Deliverable title	Data management plan (DMP)
Authors	Kovács, Gyöngyi (Hanken School of Economics)
Due date	30/06/2024
Submission date	28/06/2024
Type of deliverable	R
Dissemination level	PU

Funded by the European Union

REVISION TABLE

VERSION	CONTRIBUTORS	DATE	DESCRIPTION
V0.1	Kovács, Gyöngyi (Hanken School of Economics)	10/05/2024	First draft
V0.2	Qingbo Xu (Hanken School of Economics)	07/06/2024	Comments from Hanken's ethics and data management services
V0.3	Margot Rocheteau (Hanken School of Economics)	20/06/2024	Updated non-technical summary
V0.4	Gyöngyi Kovács (Hanken School of Economics)	24/06/2024	Added appendices and cross-checked the text
V0.5	Sarah Joseph (KLU)	27/06/2024	Updated text in 2, 2.2, 2.3, 2.4
V0.6	Duc Trinh Tan, Seng Kiong Kok (RMIT VN)	27/06/2024	Updates in sections 2.2, 2.4 and 6.2
V0.7	Jaime ter Linden (Solvoz)	27/06/2024	Updates in section 3.2
V0.8	Shadrack Opon (PSA)	27/06/2024	Updates in section 6.2
V0.9	Nadine Mellem (Innovation Norway)	27/06/2024	Cross-checking section 2
V1	Gyöngyi Kovács (Hanken)	28/06/2024	Final version for submission

LIST OF ACRONYMS

ACRONYM	FULL NAME
CLD	Causal loop diagram
DMP	Data management plan
DoA	Description of action
DPA	Data processing agreement
DPIA	Data protection impact assessment
DPO	Data protection officer
EC	European Commission
EU	European Union

Funded by the European Union

FAIR	Data are findable, accessible, interoperable, and reuseable
GDPR	General Data Protection Regulation of the EU (2016/679)
HEU	Horizon Europe
HNPW	Humanitarian Networks and Partnerships Weeks
IPR	Intellectual property right(s)
LCA	Life cycle assessment
WORM	Waste in humanitarian Operations: Reduction and Minimisation
WPs	Work Packages
WPL	Work package leader

TABLE OF CONTENT

BACKGROUND ABOUT WORM

WORM aims to design guidelines and support actions for circular economy in the humanitarian sector. It integrates bio-based technological solutions, leverages procurement for waste reduction, improves waste management methods and prioritises the sustainable livelihoods of waste pickers. WORM focuses on two selected settings: field hospital deployments and humanitarian livelihood programmes with a waste picking component. Following a collaborative and multi-actor approach, WORM brings together medical and humanitarian organisations, procurement service providers, logistics providers, waste management services and academic partners.

EXECUTIVE SUMMARY

This document is a deliverable of the WORM Project, funded under the European Union's Horizon Europe research and innovation programme under the grant agreement No 101135392.

The aim of this document is to establish WORM's data management plan (DMP). The DMP builds on the principles of FAIRness, transparency and accessibility, taking EU and different national obligations into account. The DMP identifies all data collected, processed and/or generated by the project, analyses their main generators and users, and defines how data is handled during and after the project. It details the organisation, description, storage, sharing, and publication of the research data used in this research project, and specifies the key actions for ethical and legal compliance and FAIR data production. It describes the data management life cycle according to the HEU DMP template.

D9.2 is the first version of the DMP, which will be followed by updates in WPL meetings. Revisions are sent to the EC as appropriate.

NON-TECHNICAL SUMMARY

This Data management plan (DMP) is a guidebook which describes how the WORM project handles research data. It describes the essential properties of the research data used in WORM, measures for maintaining high ethical standards and complying with relevant legislation, data ownership and access rights, planned lifespan of the data, and a plan for publishing the data in line with the FAIR data principles.

The DMP describes how data is organised, described, stored, and shared. It identifies all data collected, processed or generated during and after the project. The DMP has set out guidelines for the consortium on how to safely and securely handle personal data in accordance with the national and EU ethics and legal requirements including the General Data Protection Regulation (GDPR), and developed provisional guidelines on how to implement the FAIR principles to the datasets.

All research partners are responsible for complying with good data management practices and guidelines on the management and sharing of research data, data security and data protection in accordance with relevant legislation and research integrity. At the same time, researchers shall ensure the transparency and reusability of research materials produced and used in this project in line with the FAIR data principles.

The DMP as a living document will be updated and enriched as the project evolves.

1. INTRODUCTION

This document is a deliverable of the WORM Project, funded under the European Union's Horizon Europe research and innovation programme under the grant agreement No 101135392. This deliverable, corresponding to task 9.3, presents WORM's data management plan (DMP) and is the second output from Work Package 9 (WP9). Led by the Hanken School of Economics (Hanken), WP9 focuses on the project management of WORM, including data management.

The DMP delineates the essential aspects of collecting, processing, storing, sharing, and publishing the data in WORM. It builds on the principles of FAIRness, transparency and accessibility, taking EU and different national obligations into account. The DMP identifies all the data collected, processed and/or generated by the project, analyses their main generators and users, and defines how data is handled during and after the project. It describes the data management life cycle according to the HEU DMP template, as well as ensuring that robust protocols for data security are established to safeguard personal information (in line with the GDPR), maintaining data quality as well as confidentiality. Equally important, the DMP identifies the key actions for FAIR data production, ensuring the findability and citability of the research data according to the FAIR data principles, while sees to that the degree of data openness and sharing is ethically and legally justifiable.

The aim of the DMP is thus to be a description of the datasets within the WORM project, but also to provide guidelines on data management to the WORM consortium. The guidelines defined in this DMP shall be followed by the WORM consortium to ensure that research data are collected, transferred, analysed, shared or otherwise processed in a secure setting, that use of the data is compliant with ethical and legal requirements, and that the openness, discoverability, and reusability of our research data are promoted as much as possible. The DMP starts with a general description of the data processed in the project (Section 2). Section 3 discusses the implementation of FAIR data principles. In Section 4, guidelines are provided for the consortium on the allocation of resources. Section 5 describes how to ensure data storage, backup, transfers, and archival in a secure way. Section 6 elaborates ethical issues involved in the project and identifies the key measures for ethical and legal compliance. Section 7 outlines the legal aspects of data management.

While D9.2 is the first version of the DMP, it has resulted from discussions about data management with the consortium already during the project proposal, at the kick-off meeting in M1 (Jan 25, 2024), for and during the ethics clearance process in M1-M2, and at the WORM general assembly meeting at the Humanitarian Networks and Partnerships Weeks (HNPW) in M5 (May 7, 2024). D9.2 will further be followed up during WPL and general assembly meetings. The DMP is a living document that accompanies the whole research data life cycle, extending also after the active phase of the research project. An updated DMP (D10.1) is set to be delivered at M16, capturing any updates between the first and second periods of the project.

2. DATA SUMMARY

WORM collects data from different sources to be able to fulfil the aims of the project. WP1 commences with a scoping exercise including all WORM parties (beneficiaries and associate partners) and collecting data for various WPs. The scoping exercise focuses on three main subsets of data: identification of relevant product groups for bio-based alternatives; baseline data on waste streams and waste treatments, and baseline data on procurement practices. The data collected from the first two subsets (identification of priority products and baseline data on waste treatments) will also be used to feed into the second part of WP1, where Life Cycle Assessment (LCA) is used to capture the environmental impacts associated with producing and treating the identified products at the end-of-life according to conventional and bio-based scenarios. Thereby WP1 establishes a common baseline for other WPs as well. Joint data collection for all

Funded by the European Union

WPs ensures that the project establishes a common view, and that the data complements one another in a way that answers WORM's research questions. Since various types of data are needed from the same organisations, joint data collection also ensures that the project speaks with one voice and that the data collection becomes a concerted effort rather than fragmented across various WPs. Furthermore, this creates the opportunities for the reuse of data across the project.

This section provides a general description of the data collected and generated in the project and of the purpose of the data collection/generation, data types and formats, secondary data reused, origin of the data, data size, and data utility.

2.1 Purpose of the data collection/generation

The primary purpose of the data collection/generation in WORM is to gather insights and information relevant to the project's objectives. WORM's overall objective is designing guidelines and support actions for circular economy in the humanitarian sector. WORM focuses on two selected settings: field hospital deployments, and humanitarian livelihood programmes with a waste picking component. Across these settings, the project focuses on several cross-cutting focus areas:

- the integration of bio-based technological innovation solutions in the humanitarian context,
- using procurement as a gatekeeper for waste avoidance, and gateway to integrate innovative solutions,
- improvements in waste management, and the use of less polluting waste treatment methods,
- a specific focus on the sustainable livelihoods of waste pickers, and
- policy development, advocacy, and a heightened local awareness of improved WM in the relevant local contexts.

2.2 Data types and formats

To design guidelines and support actions for circular economy in the humanitarian sector, the WORM project engages in data collection from primary and secondary sources. This involves obtaining qualitative data through surveys and interviews with experts in the field, in addition to quantitative data from suppliers and waste management practitioners to carry out the LCAs. Expertise is needed across various areas: production, procurement, innovation, waste management and waste treatment, and across two distinct settings: field hospitals and clinics; and livelihoods programmes.

WORM data comes in the types and formats of:

- quantitative and qualitative survey data in .xlsx,. .csv and .txt formats,
- interview data (semi-structured interviews, focus groups), audio recordings in .mp3 and .wav, transcripts in .docx, .txt, .pdf
- quantitative data from ERP systems and waste management systems, in .xlsx, .csv, .pdf
- secondary waste stream data from field hospitals / clinic deployments, in .docx, .txt, .xlsx, .csv, .pdf
- process descriptions (e.g. procurement processes, waste treatment processes), in docx, .pdf, .jpg, .png, .xml, .ppt, and
- policy documents in .pdf and .ppt formats.

In other words, WORM data includes procedural data, quantitative data on product groups and their respective waste streams; quantitative data on inputs for production and waste management; surveys; audio data from interviews, as well as text data from documents and interview transcripts. This is complemented by figures drawn in workshops and seminars.

Funded by the European Union

Preference has been given to open, standard, and non-proprietary data formats to facilitate common usage and long-term reuse of the data. File types and formats are determined in a way that enables data sharing and interoperability with existing systems and co-ordination platforms, etc. At the end of the project, the pseudonymised data[1] will be deposited into the open platform Zenodo in non-proprietary formats (e.g., plain text).

2.3 Existing data reused

Besides data collected from surveys and interviews, WORM combines and reuses publicly available data (e.g. policy documents, data from scientific literature for the LCAs and CLDs), and data from the systems of WORM end users:

- quantitative data from ERP systems and waste management systems,
- secondary data from scientific literature,
- secondary waste stream data from field hospitals / clinic deployments,
- process descriptions (e.g. procurement processes, waste treatment processes), and
- policy documents.

2.4 Origin of the data

WORM uses publicly available open data as well as collects primary data from various respondents and stakeholders. Primary data is collected, using social scientific methods, in particular semi-structured interviews and focus group interviews. Respondents are human subjects, from whom data is collected by means of direct interaction and/or observation.

In the context of WORM, a research participant engages directly with the project by answering questions in an interview. The data is collected via interviews and surveys, and other stakeholder engagement activities for transcription and further analysis. In some cases, the data will be transcribed with automate methods which are encrypted both in transit and at rest and only the account owner has access to and control over the data.

Data collection procedures used include:

- documents and process descriptions collected from WORM end users
- policy documents from WORM end users and donors
- waste types and quantities from waste audits or field hospitals / health care centres studied
- expert interviews
- surveys with suppliers and waste management experts
- focus groups with people in waste management
- stakeholder workshop

Expert interviews, focus groups, and stakeholder workshops are accompanied by the WORM privacy notice/Annex 2 and informed consent/Annex 3 forms. Analysis methods include thematic analysis, procedural analysis, life cycle assessment, waste stream analysis, and causal loop diagrams.

2.5 Data size

Data size varies depending on the data types:

[1] Acknowledging that full anonymisation is not possible, the project uses the term “pseudonymisation” and applies pseudonymisation methods.

Funded by the European Union

- survey data, usually <1MB files each,
- interview data, <1-2 MB files each,
- quantitative data, <1-20 MB files each,
- secondary waste stream data from field hospitals / clinic deployments, <1-20 MB files each,
- process descriptions, 10-20 MB files each,
- policy documents, 5-20 MB files each.
- pictures, figures, <5MB files each.

2.6 Data utility

The research data can be useful to the principal stakeholder categories targeted by WORM's dissemination and communication activities:

- professionals in field hospital deployments and humanitarian livelihood programmes with a waste picking component,
- waste pickers,
- government (local, national, EU, other) including public authorities,
- (medical) humanitarian sector,
- Industry (suppliers and service providers to the humanitarian sector),
- research community,
- media, and
- the general public.

3. FAIR DATA MANAGEMENT

3.1 Making data findable, including provisions for metadata

To make the data easily findable, the project will archive the digital data in Zenodo and use descriptive metadata as required and provided by the data storage repository.

The research project will also make sure that properly documented metadata of research data is published by using the Fairdata Qvain metadata tool. Qvain is part of the Fairdata services to support research data to go FAIR. The services are offered by the Finnish Ministry of Education and Culture and produced by CSC – IT centre for research in Finland. The open research data and associated metadata will be assigned unique DOI (digital object identifiers) in Zenodo and Qvain, which enables (meta)data uniquely identifiable, and thus accessible and referenceable. Data will further be documented in a readme file to ensure that it is fully and correctly interpreted.

Metadata will include content about data title, creators, contact information, dates, data subjects/keywords, funders, licenses, languages, geographic locations, abbreviations or codes used in the dataset, methodology used in data collection/generation, instrument and protocol information, survey tool details, and version information. Properly describing and documenting data enables users, as well as the research members, to understand and track important details of the research, and facilitates data search and retrieval in the data repository.

Files and folders will be versioned and structured by using a name convention consisting of project name, dataset name, and version information. The WORM project management handbook (D9.1) has defined the naming conventions for documents including the coding of release numbers as follows:

For deliverables, the file name must start with WORM and contain the following elements as a minimum:

- WORM-Dnumber_Short-Title_VersionNumber

Funded by the European Union

- Example: WORM-D9.1 project management handbook v1.0.pdf

The WORM SharePoint is set up to automatically save revisions, and it is paramount that people adding to the document also note their names and what they have altered in the revision table in the beginning of the document. New release numbers are used for major changes only.

For all other project documents, the file name must start with WORM and contain the following elements as a minimum:

WORM-Title_ReleaseNumber

Example: WORM-kick off agenda 25.1.2024

Where:

- WORM: the project acronym
- Kick-off agenda: title of document
- 25.1.2024: release number / date

Search keywords and subject headings from the KOKO Ontology (integrated in the Qvain metadata tool) will be provided to optimise data reuse possibilities.

3.2 Making data openly accessible

As already specified in the WORM grant agreement, open science (OS) principles are key both for the project and the community behind it. OS is the key idea guiding scientific dissemination in WORM. The WORM consortium encourages early sharing of research outputs (data and publications) in an open, transparent, and re-usable fashion, contributes to increasing the quality of research results and maximises the impact for society. OS is a key part of the research design of the WORM proposal. During the last years, the OS policy of the European Commission has been designed around eight ambitions, set by the Open Science Policy Platform19 in 2020: (1) Rewards and Incentives; (2) Indicators & Next-Generation Metrics; (3) Future of Scholarly Communications; (4) European Open Science Cloud (EOSC); (5) FAIR Data; (6) Research Integrity; (7) Skills & Education; (8) Citizen Science. Each of these ambitions affects the modus operandi of research funding agencies, research performing institutions, entities responsible for scholarly communication, and research evaluation agencies. The eight ambitions are taken into consideration for the work throughout WORM's project cycle: data collection, analysis, recommendations, and validation. WORM implements open, transparent, and reusable methodologies, and documents them to ensure replicability. All research data collected and/or processed during the project length follow a creating-processing-analysing-preserving-giving-access life cycle.

WORM's commitment to open science practices leads to the plan for specific data management actions. The issue of FAIR principles guide data collection procedures in all WPs. WPL will be involved from the very beginning of the project in order to define how to implement the 'FAIR' approach defined by the EC ("findable, accessible, interoperable and re-usable"). The consortium will work towards releasing the data used, collected, processed, and generated in the open platform Zenodo. The WORM project can be found on Zenodo at https://zenodo.org/communities/worm_eu/

With the research participant's permission, after all direct identifiers are removed and indirect identifiers removed or categorised, data collected during the course of the project will be made openly available on the project website, in presentations at conferences, in the project deliverables, and in journal and practitioner articles. Data in the pseudonymised form will be submitted to and archived in Zenodo in accordance with their services, for the purpose of allowing other researchers as well as scientific publication outlets to conduct further scientific analyses on the data. Any part of data with personal identifiers and/or geolocations or for which a respondent has not consented to its archival will not be submitted for archival.

Funded by the European Union

All tools, software, and components in WORM needed to use the raw data to validate research results will be available as open source under appropriate licences. There will be no restrictions on use and access to the open data. Separately, access to, and the use of software, tools and platforms that constitute background are noted the consortium agreement, which stipulates their licencing agreements and duration of licences to the duration of the project. See section 7 for the legal aspects of the project.

3.3 Making data interoperable

All data processed in the project will use non-proprietary formats with standard representations (Unicode) and meet the requirements: non-proprietary; open, documented standard; common usage by research community; standard representation (ASCII, Unicode); and uncompressed.

When depositing data in Zenodo, the project will ensure that the research data is migrated to new formats, platforms, and storage media as required by good open science practices to enable data sharing, reuse, and interoperability between researchers, institutions, organisations, and countries, while commonly used, non-proprietary, and parsable file formats have been selected to support the interoperability of the data.

Crucially, all WORM outputs are designed to be cost-effective and open source as far as privacy allows, thereby supporting those organisations where resources may be limited and ensuring data reuse and interoperability. Standard, controlled vocabularies will be used for describing all variables, and for labelling, indexing or categorising datasets. Furthermore, the WORM project will use common social science data collection methods and practices, which also contributes to data interoperability.

3.4 Increase data re-use (through clarifying licences)

The consortium will save the pseudonymised data in a non-proprietary format (e.g., plain text) and deposit them into Zenodo after the data has been cleaned and pseudonymised. Good practice developed by the Zenodo team can ensure the ongoing integrity and validity of the data deposited.

A creative commons license CC-BY (requiring attribution) or CC-0 (no rights reserved) will be used for all of WORM's document-based outputs (e.g., deliverables) and open research data, free of charge for any user and without any embargo period, to ensure that they are shared with minimal restrictions, aside from attribution to the authors or creators. The project's outputs will be made available on the WORM website and/or through open access publications. The documents will be available under a CC BY licence and the data will be available as public domain (CC0) to facilitate reuse. Data will be described with rich metadata, and registered or indexed in searchable resources wherever possible. The resources will also be linked with OABT entries to encourage findability and reuse.

Regarding its DCE activities, WORM engages and involves the WORM consortium and identified stakeholders in the co-design and co-creation of the project outputs, thus promoting OS practices and responsible research and innovation values through its open validation process. Amongst the dissemination activities, WORM consortium members will produce academic/research papers that will be published in Open Research Europe (ORE) or in open access scientific journals and shared in Zenodo, under a CC BY licence. Authors will retain the intellectual property rights to comply with the open access obligations of Horizon Europe, persistent identifiers in the publications will be used (like ORCID for authors, and the Funder Registry for the EC as the funding agency), and the name of the action, the acronym, and the grant number amongst the metadata will be referenced. Authors will guarantee that metadata will be provided as a public domain dedication (CC0) both in the journal and in the open access repositories where they are archived. Underlying research data will be linked to the publications through their DOIs, and will be published under the principle of 'as open as possible and as closed as necessary', and pseudonymise any identifiers, and published either in the same journal, when possible, or in Zenodo as CC0 thus making them follow the FAIR20 principles. Target journals will be selected based on OS

Funded by the
European Union

principles. For example, the Journal of Humanitarian Logistics and Supply Chain Management, has a new OS policy without any fees to authors. In all cases, gold open access is targeted.

To ensure the quality and consistency of the data, transcriptions of audio interviews will be checked by someone other than the transcriber/transcription service provider, analogue materials be digitised in as high resolution as possible for accuracy, and dates of data collection, retrieval, and changes be recorded, making all data related actions traceable and repeatable. Data protection measures such as minimisation, pseudonymisation, and pseudonymisation will not affect data quality. In all conversions, maintaining the original information content will be ensured.

4. ALLOCATION OF RESOURCES

The project PI is responsible for the initial planning and execution of data management procedures, and all WPLs for the implementation of these procedures. All researchers working for the project are responsible for the tasks of data collection, data storage and backup, data documentation and sharing, and all consortium members and their team members are expected to comply with this data management strategy including related legislation. Potential new team members will be fully informed about this strategy and requested to adopt all its rules before starting their work in the team, and find all relevant material on the WORM SharePoint. In WORM, data management is reviewed internally, at the respective institutional levels of research organisations, and also externally by an independent ethics consultant. The next external ethics review is at the end of the first interim period of the project. The DMP itself is updated for a next deliverable, D10.1 for the second interim period of the project. The PI being at Hanken, Hanken's research support unit provides assistance with data management and management of IPRs.

In the following sections, guidelines are described for research partners to follow in case of datasets with personal data. All research partners ought to follow these guidelines and procedures, and bear the responsibilities for legal, ethical, and moral concerns and decisions involved in the research and during the interaction between the researcher and research participants. For each dataset, a responsible person has been appointed at the partner level, who will be held accountable for this specific dataset. All researchers shall describe their datasets containing personal data and share the description with the data protection officer (DPO) at their own organisation, in line with the GDPR (Art. 24, 28).

The research project has also allocated time and budget to complete the data management tasks and cover relevant costs. Archival in the repository Zenodo and metadata production through Qvain are both free of charge. The data management tasks altogether will accompany the entire project throughout.

WORM does not consider the long-term preservation of the research data. Research data will be preserved internally at least until the publications from WORM are under process, and externally on Zenodo.

5. DATA SECURITY

WORM agrees on and disseminates the joint data security guidelines to all research partners to ensure that data is securely stored and managed. Besides each institution's data security instructions, the research team members shall follow these joint rules of the consortium. Appropriate technical and organisational measures are implemented to ensure data security and prevent risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data. In case of a security incident, the DPOs will work closely together with data security officers of the participating universities.

For secure data storage and backup, the WORM consortium stores the information received from interviews, workshops, surveys, etc., in password-protected personal computers (company computers for personal use) and a joint secured SharePoint (based within Hanken's Teams) with appropriate security

Funded by the European Union

restrictions in place. This includes access restrictions to IT systems and storage such as password protection, encryption, etc., by complying with all national and EU legislations. Hanken-provided systems do automatic backups. Data is retrievable in case of human error or data corruption. In addition, manual backups of master data files are taken regularly and always before any major file-format or data conversions.

For secure data transfers, sharing of transcripts across the consortium members that need access to the data for various types of analysis is only via the joint SharePoint. Closed channels on Teams are created for data that is still being processed for pseudonymisation.

Special attention has been paid to the GDPR when handling data from non-EU countries. Field research has been carried out in Kenya and Vietnam. Researchers are deployed with humanitarian organisations that are experienced in these environments. Their security protocols and duty of care apply. Furthermore, many of the researchers are members of rosters of humanitarian organisations and have themselves experience from previous deployments, and the necessary security trainings for these.

After data has been collected in Kenya and Vietnam, it is translated and transcribed by local transcription/translation service providers in the same country, and then uploaded to the WORM SharePoint under the WP for which it was collected. The files in the recorders are then irretrievably deleted. Rights to access the data and data usage are then controlled by the PI with the support of the project management office. The PI completes the list of users and all rights granted, and a procedure for withdrawing rights. Access to data is only granted to authenticated research members of the project. Access to the identifiable data will be restricted to those researchers directly involved in the project.

WORM partners outside the EU involved in data analysis (RMIT Vietnam, PSA) have access to the pseudonymised data in the shared secure WORM SharePoint. No personal data is transferred outside the EU/EEA or to international organisations, and personal data processing and transfers only reside inside the EU/EEA and are limited to the research. Access control is in line with the level of confidentiality involved. Personal data is protected with adequate, appropriate safeguard measures such as encryption and strict access control, and will not be sent between research team members by email or other types of file transfers.

The project enters into agreements including a data processing agreement (DPA) and/or a non-disclosure agreement with all service providers who conduct translation/interpretation or transliteration/transcription work which contains any personal or individual-specific data or is based on any individual informants. The WORM SharePoint is covered by Hanken's DPA with its service providers. The consortium's data processing agreements are covered by the WORM consortium agreement that all beneficiaries have signed.

The pseudonymised data will be archived into the certified, trustworthy data repository Zenodo.

6. ETHICAL ASPECTS

6.1 Data protection

The participation of different types of stakeholders in WORM's activities means that personal data, or data that can identify participating stakeholders, are collected by members of the consortium. Data is collected from expert interviews, focus groups with people in waste management, and stakeholder workshops, combined with secondary data from ERP systems and waste management systems, field hospitals / clinic deployments, process descriptions, and policy documents. Personal data can be found in the survey data and audio data from interviews with professionals in humanitarian organisations and

Funded by the European Union

waste treatment organisations, hospital waste management staff, people involved in waste management, and procurement experts.

The project co-ordinator acts as the data controller who ensures that WORM's activities are compliant with EU rules and regulations. The co-ordinator Hanken has appointed a Data Protection Officer (DPO) from whom project WORM obtains advice about data protection obligations and how to meet them. The DPO's contact details are given to all the data subjects involved in the collection and processing of the above-mentioned personal data types, as well as of the secondary data type if applicable. All research partners and service providers follow relevant ethical and legal requirements and implement WORM's technical and organisational data protection measures.

WORM specifies that the following direct identifiers – name, e-mail address, facial image (e.g. picture, video footage showing the face), voice recording – can be collected from the respondents and stored encrypted on the WORM SharePoint until transcribed and pseudonymised, where they are safely managed according to the DMP. Separate questions are asked from respondents in the informed consent sheet about each of these aspects, as well as in the recording of webinars.

WORM will have a mailing list that respondents and other stakeholders can sign up for. This is upon their own discretion. The mailing list is for the purposes of dissemination in the project and is not used for cross-identifications with respondents. Only the dissemination partner (Euronovia) maintains the WORM mailing list. The collected contact information of research participants which is not linked to files containing other personal data, is stored securely in a separate shared file with restricted access.

Even though WORM focuses on a field hospital setting, data is collected from experts through interviews and surveys, from ERP systems, from waste streams, and in forms of documents, but not from patients. WORM does not collect any medical data of any respondents. No special categories of personal data (sensitive personal data, GDPR Art. 9-10) such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal offences, genetic data, biometric data processed solely to identify a human being, health-related data, data concerning a person's sex life or sexual orientation, and personal data relating to criminal convictions and offences or related security measures, and no data of a highly person will be involved in the project.

If a data subject by own initiative discloses sensitive data to the representative of the project, such information should be by default not be stored or transferred further. In case a member of the WORM team would intentionally or unintentionally be given access to any form of sensitive data, is the person obligated to a strict non-disclosure and to absolutely refrain from any ways to use, transfer, store or exploit the sensitive data.

Data of interest to WORM relate to materials and their adequate waste management, to procurement and to innovation. Data that is not relevant for the project will not be asked about. If any such data comes up in an interview, it will be removed in the pseudonymisation process.

To respect and protect the fundamental rights of the data subjects, the WORM project adopts adequate technical and organisational measures for data protection by design and default and monitors continuously if these measures are implemented appropriately to ensure that ethical standards and guidelines within Horizon Europe and all relevant national and European legislations are rigorously applied, regardless of where the research is conducted. The consortium has performed a data protection impact assessment (DPIA, Annex 1) and will keep records of all data processing activities. WORM's DPIA was filed in February 2024, approved by Hanken's Data protection officer (DPO) on May 7, 2024. It was made available to the WORM consortium on the WORM SharePoint on May 8, 2024. Policies and procedures have been established about how to limit the use of data and minimise data collection, how to inform the data subjects, how to pseudonymise or anonymise data wherever possible, how to deal with complaints and data breaches, and how to perform data erasure within the specified time periods. WORM identifies the legal basis for personal data processing and ensure that adequate level of protection and

Funded by the
European Union

appropriate safeguards are applied during data storage, transferal, sharing, and preservation. The project enters into agreements including a data processing agreement (DPA) with all service providers. The WORM SharePoint is covered by Hanken's DPA with its service providers. The consortium's data processing agreements are covered by the WORM consortium agreement that all beneficiaries have signed.

Data protection by design is implemented in practice during the active research phase in the following aspects:

- **Clarify the legal basis for processing**. The purpose of the dataset and legal basis for data processing in this project is scientific research carried out in the public interest. In addition, in accordance with ethical standards, project WORM asks for informed consent of the research participants when collecting and processing personal data, as well as secondary data if applicable. Respondents can withdraw their consent at any time. Consent for using material for communication purposes is obtained separately (separate point respondents can opt in for).
  If it is unrealistic to get informed consent sheets (plan B only), research members ask twice for consent in an interview: once before asking whether recording can be made, and then repeat the question on recording. All signed consent sheets are kept on file and stored with the data under each WP and can be provided upon request.
- **Inform the data subjects with sufficient information on the processing of their personal data.** The project will use Hanken's e-form privacy notice. Each respondent will receive such a privacy notice prior to data collection. The privacy notice describes what personal data will be collected from each respondent as a participating individual, and why and how the personal data will be processed in the research, as well as the details of the research project and related participation. It also provides information on what rights each respondent as the data subject has pertaining to the personal data and how s/he can exercise these rights in relation to the processing.
  For ensuring the enforcement of data subjects' rights, all research partners will provide privacy notice to each participant and ask for informed consent from each of them. Joint and shared measures and arrangements are made to enable data subjects to fulfil and exercise their fundamental rights.
  The informed consent (Annex 2) and privacy notice (Annex 3) that research participants are provided to read and accept are attached in this DMP.
- **Keep records of data processing activities.** Records of data processing activities by both the data controller and data processors are drawn up and kept on file, and can be, if needed, accessible to data subjects, research funder/Commission services, or data protection supervisory authorities.
- **Sign a data processing agreement (DPA).** All data processors who conduct translation/interpretation or transliteration/transcription work, which contains any personal or individual-specific data, or are based on any individual informants shall sign a data processing agreement (DPA). The WORM consortium agreement covers the data processing of research partners.
- **Implement data minimisation.** WORM's data protection policy implements the principles of purpose limitation and data minimisation in a comprehensive way, covering research, education, infrastructure, and partnerships. Project WORM only collects and processes data that are necessary and proportionate to achieve the tasks of this project. Personal data will only be processed for the scientific research purpose and will not be used for any other purposes that are not considered to be compatible with this original scientific research purpose.
  A data minimisation review has been conducted by the research partners at the meeting at HNPW 2024 for the whole process of data management, including defining the amount of personal data collected, the extent to which they may be accessed, further processed and shared, the purposes for which they are used, and the period for which they are kept.

Funded by the European Union

- **Pseudonymise the data wherever possible.** Pseudonymisation is performed as soon as possible, for instance, right after the data has been aggregated and before data analysis to protect the data subjects' privacy and minimise the risk to their fundamental rights. The additional information on the original values and techniques used to create the pseudonyms or codes is kept organisationally and technically separately from the pseudonymised data to ensure that the personal data are not attributed to an identified or identifiable natural person.
  Interview transcripts, documents, and procedural data obtained from various stakeholders in the consortium are pseudonymised for data analysis. Names for first identification have been pseudonymised to position, expertise, type of organisation, and country. As agreed in the meeting at HNPW2024, **the pseudonymisation key includes country, type of organisation, expertise, date, e.g., KEHUMWM20240607. Three types of country denominations will be used: KE (Kenya), VN (Vietnam), and ROW (rest of the world).** A key of the informants is kept separately from pseudonymised transcripts but use the same pseudonyms in both.
  Any data with personal identifiers will be pseudonymised before sharing and data analysis. Any organisation-specific numerical and procedural data that is collected will also be pseudonymised in all deliverables and publications.
- **Ensure data security.** Appropriate technical and organisational measures are implemented to ensure data security and prevent risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data. See 5. Data security.
- **Data from and to non-EU countries.** The research team members rigorously maintain high ethical standards and comply with relevant legislations, regardless of the country in which the research is carried out and data are collected and processed. Project WORM ensures that when collecting personal data outside the EU and when transferring personal data from a non-EU country to the EU (or another third state), data processing activities fully comply with the EU legislations and national laws of any country in which the research is conducted and the data collected. After personal data has been collected in a non-EU country, it is translated and transcribed by local transcription/translation service providers in the same country, and then uploaded to the WORM Teams under the WP for which it was collected. The files in the recorders are then irretrievably deleted. No personal data will then be transferred outside the EU/EEA or to international organisations, and personal data processing and transfers only reside inside the EU/EEA and are limited to the research.
- **Data erasure and data sharing.** The WORM project makes sure that personal data, dispensable data files, temporary files created when programs are used, and all their back-ups shall be deleted within due time when they are no longer needed, and that the deleted data cannot be recovered. All the personal data will be erased within five years after the completion of the research project. With the research participant's permission, the consortium will share and archive the pseudonymised data in Zenodo for any users to access, mine, exploit, reproduce, and disseminate free of charge.

6.2 Ethical dimension of the objectives, methodology and likely impact

WORM focuses on waste management in the humanitarian context. By introducing alternative bio-based products and materials, it seeks to reduce environmental damage, but it may impact negatively on livelihoods. WORM elucidates such potential negative implications in a causal loop diagram. Different alternative waste treatment methods and their environmental impact are studied in the project.

The humanitarian context targets most vulnerable populations. Even though workshops will be held for vulnerable populations (e.g. waste pickers), no data will be collected from these, but instead, from humanitarian organisations. WORM adheres to all humanitarian principles which include humanity (and thereby non-discrimination), and impartiality.

Funded by the European Union

Vulnerable populations (esp. waste pickers) will be targeted through local awareness campaigns. Campaigns will engage waste handlers, community groups, county representatives, health workers, and teachers, who in turn can include campaign materials at schools. WORM will head the advice of its humanitarian end users before engaging with any vulnerable populations. In all data collection, and in the local awareness campaigns, active informed consent will be sought. Participation in the project is at all times fully voluntary, and participants have the right to withdraw and terminate their participation.

WORM's use case setting of field hospitals includes a focus on medical, and thereby potentially toxic and hazardous waste. The project focuses inherently on the development of less toxic waste treatment practices and engages scientists familiar with safety and hygiene precautions in their evaluation.

WORM includes project members from low- and middle-income countries. They play an important role in the implementation of the project and in the organisation of local awareness campaigns. They, and several other members of the WORM consortium, are engaged with Horizon Europe project for the first time. Therefore, WORM is implementing the system of work package leads with co-leads, actively building the capacity of its consortium to implement such projects.

6.3 Compliance with ethical principles and relevant legislations

All of WORM's activities are compliant with EU rules and regulations. Waste management legislation and treatment possibilities differ across WORM implementation countries. This is in fact one of the focus areas of WORM, seeking to improve waste management practices, evaluating alternatives, and running local awareness campaigns for their improvement.

WORM adheres to the Vancouver protocol with regards to publications, co-authoring, and rights to data and publications, and follows the guidelines and best practices of the Finnish National Board on Research Integrity (TENK). WORM's research protocol has been approved by Hanken's research ethics board on Feb 21, 2024. The development of data collection instruments and the data management plan are guided by Hanken's research ethics board and Data protection officer.

Further ethics issues were identified as a result of the ethics evaluations. These are dealt with under WP11. An external independent ethics advisor has been appointed for this purpose and will submit a report at the end of each reporting period. The project, and the report, shall pay attention to

- A data management plan for personal data, the processing and sharing of such data and the time period of its retention.
- The potential biohazard risks connected with dangerous waste coming also from hospitals and vulnerable populations.
- The potential geopolitical risks for research staff when working in potentially unstable countries.
- The safety rules for research staff, as shall be elaborated on and agreed on at the beginning of WP7.

The Consortium confirms that compliance with ethical principles and applicable international, EU and national law in the implementation of research activities not originally envisaged (or not described in detail) in the DoA will be ensured. The Consortium also confirms that any ethical concerns raised by those activities will be handled by following rigorously the recommendations provided in the European Commission Ethics Self-Assessment Guidelines.

7. LEGAL ASPECTS

The WORM grant agreement and consortium agreement cover all legal aspects of the project. This includes agreements on authorship, ownership, access rights, exploitation, dissemination, and IPR. The consortium agreement further specifies the structure of the project, and accordingly, sets that the WORM

Funded by the European Union

General Assembly as the highest decision-making body of the project that makes consortium-level decisions including any potential requests for changes to these agreements. As stipulated by the WORM project management handbook (D9.1), all contractual documents are found on the WORM SharePoint. The terms and provisions of the grant agreement and its annexes, and the WORM consortium agreement will prevail in the event of any inconsistencies with the information and rules also in the DMP.

The WORM consortium agreement further stipulates that prior notice of any planned publication shall be given to the other Parties at least 45 calendar days before the publication. Any objection to the planned publication shall be made in accordance with the Grant Agreement by written notice to the Co-ordinator and to the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice. If no objection is made within the time limit stated above, the publication is permitted. For the case of any disagreements, conflict resolution mechanisms are detailed in the WORM project management handbook (D9.1).

IPR rules conform to HEU regulations and principles. Authors will retain the IPRs to comply with the open access obligations of Horizon Europe. When reusing secondary data gathered from open sources, good practices for the attribution of authorship and data citation will be followed, and all legal restrictions such as copyright permissions and license terms on its use observed.

WORM ensures the exploitability of its results while contributing to open standards development. Access rights to results or background that are needed for exploitation are also agreed on in the WORM consortium agreement.

Funded by the European Union

ANNEX 1 Data Protection Impact Assessment (DPIA)

1. Data protection impact assessment (DPIA)

1. Description of processing activities

1.1. Basic information about the research

1.1.1. Name of the research study

WORM (Waste in humanitarian operations: reduction and minimisation)

1.1.2. Principal investigator and research group

Principal investigator: Gyöngyi Kovács

Contact information: kovacs@hanken.fi

Research group or field of research: SCM&SR / Hanken as consortium lead

1.2. Scope of processing activities

Number of the data subjects (estimated): interviewees: ca. 50, workshop participants: ca. 100

Planned duration of the research study: 1.1.2024 – 31.12.2025

1.3. Categories of personal data to be processed

1.3.1. Categories and sources of personal data

[Personal data refers to any information relating to an identified or identifiable natural person. Natural persons are considered identifiable if they 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 one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Answer each of the following questions:

- What types of personal data will be processed during the research study?
- Whose personal data will be processed (groups or categories of data subjects)?
- From whom or where the personal data will be collected (sources of personal data)?

Personal data collected from the data subjects:
Name for first identification, will be pseudonymised to position, expertise, type of organisation, country
Personal data collected from other sources:
Directly from respondents; through documents of partner organisations (in the consortium)

1.3.2. Processing special category of personal data

[Special categories of personal data refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Personal data relating to criminal convictions and offences or related security measures are also, by their nature, particularly sensitive and merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedom. (GDPR (Art. 9 (1), Art. 10)

Funded by the European Union

Answer the questions:

- Will your process special category of personal data (sensitive personal data), data concerning criminal convictions or offences or data of a highly personal nature in the course of your research? If yes, answer the following questions:
    - What types of special category of personal data will be processed?
    - Whose personal data will be processed (groups or categories of data subjects)?
    - From whom or where the personal data will be collected (sources of personal data)?

Special categories of personal data, data concerning criminal convictions, data of a highly personal nature or any other specially protected personal data:
N/A – DPIA filled in due to requirement for funding organisation only. None of the above apply. After pseudonymisation, groups processed for various stakeholder categories. Data collected from experts, and stakeholders attending workshops. Sources of personal data directly from respondents.

1.3.3. Description of processing activities

[Draw up a systematic description of the nature, scope, context, and purpose of personal data processing. Consider the entire life cycle of personal data from data collection to data destruction or archival. The description shall indicate why and how personal data will be processed during your research project. Address especially the following questions:

- What are the purposes for processing the personal data?
- What is the legal basis for each processing activity?
- How will you process the personal data?
- Where will you store the personal data?
- Who will take part in processing personal data, and what are their respective roles and responsibilities?
- How will the data be shared with other stakeholders involved in the processing activities?
- What will happen to the data after your research study has been completed?]

Description of processing activities:
First recordings and interview transcripts may include names. Recordings will be deleted after transcription, (translation where necessary to English,) and the pseudonymisation of transcripts. Survey data will include respondent keys for expert groupings. Interview recordings might be shared with a commercial transcription service that will be required to delete those upon completed transcription. Transcription services and translation services will include a non-disclosure agreement. Transcripts stored for the project will be pseudonymised. Documents and procedural data will be obtained from various stakeholders in the consortium and will be pseudonymised for data analysis.

Funded by the European Union

Storage of transcripts on password-protected personal computers (company computers for personal use) and a joint secured sharepoint (based within Hanken's Teams). Sharing of transcripts across the consortium members that need access to the data for various types of analysis only via the joint sharepoint. Closed channels on Teams are created for data that is still being processed for pseudonymisation. Horizon Europe requires WORM to share data openly where possible. Zenodo has been identified for this purpose. Extracts of the data (quotes, volumes and types of waste, procedural descriptions) will be used in the analysis and in reports.

1.3.4. Codes of conduct

[Will your processing activities be carried out in compliance with specific codes of conduct as referred to in Art. 40 of the GDPR?]

Indicate the codes of conduct, if applicable:
ICRC codes of conduct apply. They are the most stringent in the consortium.

2. Necessity and proportionality

2.1. Purpose limitations

[Personal data may only be collected for specified, explicit, and legitimate purposes and may not be further processed for other purposes that are incompatible with the original purposes. Answer the questions:

- What are the specific purposes for collecting and processing personal data?
- How will you ensure that personal data will not be processed for any other purposes?]

Demonstrate adherence to the purpose limitation principle:
The purpose is to devise a list of interviewees and to be able to cross-check when snowballing that the same people are not contacted twice through the project. An informant list is kept as a separate key from the pseudonymised data. Regular informed consent forms apply, and respondents can withdraw their consent at any time. Consent for using material for communication purposes is obtained separately (separate point respondents can opt in for). WORM will have a mailing list that respondents and also other stakeholders can sign up for. This is upon their own discretion. The mailing list is for the purposes of dissemination in the project and is not used for cross-identifications with respondents. Personal data will only be processed for the scientific research purpose and will not be used for any other purposes that are not considered to be compatible with this original scientific research purpose. The research will only process the personal data that are necessary and proportionate to the accomplishment of the research tasks and execution of the research.

2.2. Data minimisation

Funded by the European Union

[Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected and processed.

How do you ensure that only relevant and necessary personal data, which you need to fulfil your specified purposes, will be collected and processed in the course of your research?]

Demonstrate adherence to the data minimisation principle:
For data minimization, the project has defined the clear, specified need for collecting personal data and will only collect the minimum amount of personal data necessary and proportionate to the accomplishment of the research tasks. The project has conducted a data minimisation review for the whole process of data management, including: • defining the exact types and amount of personal data collected, • the extent to which they may be accessed, further processed, and shared, • the specific purposes for which they are used, and • the period during which they are kept. Data that is not relevant for the project will not be asked about. If any such data comes up in an interview, it will be removed in the pseudonymisation process. Even though WORM is in the area of medical logistics, no data concerns any medical data of any respondents. Data of interest to WORM relate to materials and their adequate waste management, to procurement and to innovation.

2.3. Transparency and timely communication

[Data subjects shall be provided with sufficient information about why and how their personal data will be processed and used. All information and communications shall be provided in a concise, transparent, intelligible, and easily accessible form using clear and plain language.

- What information will you provide to the data subjects about your processing activities?
- How will you provide the information about your processing activities to your data subjects?
- When will you provide this information?]

Describe how the data subjects will be informed of the processing:
Respondents will receive a short project information sheet together with the informed consent form prior to the interview. Stakeholder workshops will have their own descriptions when inviting stakeholders to them, that explains the purpose of the workshop. The project will use Hanken's e-form privacy notice.

2.4. Consent management (if the legal basis for processing is consent)

[If you ask your data subjects to provide consent for the processing of their personal data, how will you handle the consent management process?

- How will the data subjects provide their consent?
- Is consent to the processing of personal data freely given, specific, informed and unambiguous indication of the data subject's wishes?

Funded by the European Union

- How will you record their consent?
- How can the data subjects withdraw their consent?]

Describe the consent management process if the legal basis for your processing activities is consent (GDPR Art. 6 (1)(a)):
WORM adheres to GDPR also outside the European Union. Regular informed consent processes apply. For any interview online, informed consent may be given orally at the beginning of the interview (repeating the question also for the record). Consent for the use of procedural data, documents, and quantitative data is agreed on during the request for such data. Respondents can withdraw their consent at any time and will have the relevant contact details for doing so through the project information sheet/by sending their requests to the contact person.

2.5. Storage limitation and anonymisation or pseudonymisation

[Personal data that are no longer needed for the original purpose should be disposed as soon as possible unless there are special reasons or legislation that require archiving. If it is not possible to determine the exact data retention period, specify the criteria used to determine that period to your research participants.

- How have you set a retention period for the personal data you will collect or specified the criteria for setting the retention period?
- Have you considered possible further use of the personal data when setting the retention period?
- How and when will you carry out pseudonymisation or anonymisation procedures?]

Storage limitation and pseudonymisation or anonymisation:
A separate list of interviewees / respondents will be maintained as long as interview snowballing is ongoing, to avoid duplications of contacts. Transcripts will be pseudonymised through the transcription process. Retention period of raw data until pseudonymisation, with separate key of respondents. Pseudonymised transcripts will be kept for the analysis, and shared on Zenodo after articles from the project have been published. No personal data will be shared or retained beyond the data collection process.

2.6. Data subjects' rights and exemptions

[Data subjects have the right to access to their personal data, the right to rectification, the right to erasure (the right to be forgotten), the right to restrict the processing, and the right to object to the processing of their personal data, the right not be subject to automated decision-making, and the right to be informed of a personal data breach involving a high risk.

- Describe the process for ensuring the enforcement of data subjects' rights.
- Who is identified as the contact person(s) for inquiries and requests?

Funded by the European Union

- How will you ensure that information requested by the data subjects can be provided and that their other rights can be fulfilled?
- How will you document and store requests and responses?]

Process for ensuring the enforcement of data subjects' rights:
The project information sheet/privacy notice will contain the contacts for the project that respondents can get in touch with for any of the above. For practical purposes this will include the project PI at Hanken and also a person in the case country the specific data is collected in (Kenya, Vietnam) so respondents can get in touch with the team using their own language. For ensuring the enforcement of data subjects' rights, the researchers will provide privacy notice to each interviewee and ask for informed consent from each of them. The privacy notice provides clear information on personal data processing activities, what rights the data subject have pertaining to their personal data, and how they can exercise these rights including the right to access to their personal data, the right to rectification, the right to erasure (the right to be forgotten), the right to restrict the processing, and the right to object to the processing of their personal data, the right not be subject to automated decision-making, and the right to be informed of a personal data breach involving a high risk. The project has assigned a contact person whom the participants can ask questions and send requests. All data subjects' requests will be documented and stored systematically in the project-related files.

Under certain circumstances, data protection laws allow for exemptions from certain data protection provisions. Are there exemptions that apply to your research study?

Specify the exemption:	Reason(s) for exemption:
N/A	

2.7. Integrity, confidentiality, and availability

[Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.

Describe the measures (including the information security measures) that you will take to ensure the integrity and confidentiality of personal data during the different stages of processing throughout the data life cycle.]

Integrity and confidentiality during the data life cycle:
Use of Hanken's sharepoint for the sharing of any transcripts. Hanken's servers backup functions apply.

2.8. Transfers of personal data and the recipients

2.8.1. Joint controllers

[If there are at least two data controllers who jointly determine the purposes and means of personal data processing, they are referred to as joint controllers.

Funded by the European Union

If multiple data controllers participate in the processing of personal data as joint controllers, indicate their names, contact details, their roles in the processing activities, and the contact details of their designated data protection officers (if applicable).]

Joint controllers:
Hanken functions as WORM's data controller.

2.8.2. Data recipients, third parties, and data processors (subcontractors)

[To whom the personal data will be disclosed? Will any third parties have access to personal data?

Data processor refers to a person or an organisation that processes personal data on behalf of and under the instructions of the data controller.

If data processors (such as service providers of survey, data analysis, transcription or translation services) participate in the processing activities and have access to the personal data, indicate their names, contact details, their roles in the processing activities, and the contact details of their designated data protection officers (if applicable).]

Recipients of the personal data:
WORM is a consortium project and members of the consortium that are involved in data analysis have access to pseudonymised transcripts. Only the dissemination partner (Euronovia) maintains the WORM mailing list. WORM will have a data management plan as a deliverable (month 6 of the project), and various aspects of data management and ethics are also part of the grant agreement and the consortium agreement that all consortium partners sign off on. NDAs are parts of the contracts with transcription and translation services.
Data processors and third parties:
Transcription and translation services are procured separately.

2.8.3. Personal data transfers outside the European Union (EU)/European Economic Area (EEA)

[Any transfer of personal data outside the EU/ EEA shall be carried out in compliance with the GDPR requirements.

If personal data are transferred outside the EEA, where will the data be transferred? Is the target country on the list of the European Commission's Adequacy decision? If not, what GDPR-compliant transfer mechanism (Chapter V, Art. 44-50 of the GDPR) will be applied to the transfer?

You can also state this information in sections 2.8.1-2.8.3 above based on the role of each data recipient.]

Types of personal data	Recipient	Location	Transfer mechanism
Data is uploaded on the WORM sharepoint after completing transcription and translation.	WORM partners outside the EU involved in data analysis (RMIT Vietnam, PSA) have access to the	Vietnam Kenya	Access through WORM sharepoint only

Funded by the European Union

	shared secure WORM sharepoint.		

3. Risks associated with the processing

3.1. Identifying the risks associated with personal data processing

[Assess the risks that your processing activities may pose to the data subjects, especially the risks arising from:

a) unauthorised disclosure of or access to personal data,

b) unintentional or unauthorised destruction or modification of personal data, and

c) the loss or alteration of personal data.

How would you rate the severity of the possible harm or damage if the risks are realised? How would you rate the likelihood of the risks? Potential risks include, for example:

- unauthorised re-identification of pseudonymised data or loss of control over the use of personal data,
- identity theft or fraud, financial loss,
- other social disadvantage, such as reputational damage, or
- physical harm (especially when processing special categories of personal data).

Identify measures that you can take to prevent or mitigate the risks. You can consider, for example, the following questions:

- How will you restrict access to the personal data to ensure that only individuals who need to process the data for research purposes are able to gain access?
- Where will the personal data be stored and backed up? How will you securely store the personal data to maintain the integrity and confidentiality of the data?
- How will personal data be securely transferred during different stages of the research?

Type your comments in the tables below. You can refer to your earlier risk assessment as well as the mitigation measures listed in Section 2 of this DPIA.]

3.2. Unauthorised disclosure of or access to personal data

Risk	Likelihood	Severity	Mitigation	Remaining risk[2]
Accidental loss of data	Low	Low	Ensuring prompt upload of data on secured sharepoint	Low
Member of consortium leaving	Low	Medium	Consortium management	Low

[2] This refers to the level of risk that remains after you have implemented the necessary protection measures.

Funded by the European Union

the project but retaining access to sharepoint			ensuring that access to sharepoint is kept up to date	

3.3. Destruction or unauthorised modification of personal data

Risk	Likelihood	Severity	Mitigation	Remaining risk
N/A	Select	Select		Select

3.4. Loss or alteration of personal data

Risk	Likelihood	Severity	Mitigation	Remaining risk
N/A	Select	Select		Select

3.5. Summary

Overall assessment of the data protection risks: Low risk

4. Stakeholder comments

4.1. Comments by the Data protection officer (DPO)

Data protection officer's comments:

Name: _Urpo Kaila_____

Email: dpo@hanken.fi

Date: _2024-05-07_____

> This DPIA complies comprehensively with our current best practices on data protection and the impact assessment reflects our common view on require adequate technical and organisational measures. The data subjects have also adequately been informed about their rights.

4.2. Comments by other stakeholders

Stakeholder's comments:

Stakeholder group: _____

Name: _____

Date: _____

> The planned personal data processing is not likely to result in a high risk to the rights and freedoms of the data subjects. The processing does not fulfil any of the criteria that may require a DPIA to be conducted specified by the GDPR (Art. 35 (3)), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Finnish Data Protection Act (1050/2018) and List compiled by the Office of the Data

Funded by the European Union

Protection Ombudsman of processing operations which require data protection impact assessment (DPIA).

5. Summary

The planned measures for eliminating or controlling the risks associated with the personal data processing are adequate and therefore the processing activities are not likely to pose a high risk to the rights and freedoms of the data subjects (to be filled in by the person who carries out the DPIA):

☒ Yes

☐ No

If the planned measures are not adequate to mitigate the risks associated with the processing activities, or if there are no measures that can be implemented to mitigate the risks, a prior consultation with the supervisory authority/Data protection authority (DPA) (in Finland, the Finnish Data Protection Ombudsman) is required before initiating the processing of personal data. Contact Hanken's Data protection officer (DPO, dpo@hanken.fi) for assistance with the prior consultation.

Funded by the European Union

ANNEX 2 Informed consent form

Informed consent to participate in the research of the Waste in humanitarian Operations: Reduction and Minimisation (WORM) project

☐ I have been requested to participate in the research identified above. I have received sufficient information about the research and processing of my personal data in the Privacy notice in writing (in print or electronic form) and have had the opportunity to ask questions and have my questions answered.

☐ I understand that the participation in the research is voluntary. I am aware that I have the right to refuse to participate and the right to withdraw from the research permanently or for a temporary period at any time and without giving a rea-son. Withdrawal from the research will not result in any negative consequences to me. The information collected from or about me up to the point of my withdrawal may still be used in the research.

☐ I agree that the interview with me will be recorded, and that photographs and videos be taken of me for the research's purpose. The recordings, photographs, and videos will be processed in such a way that I cannot be identified in them.

[In case the interview takes place as part of a workshop:]

☐ I agree that videos or photographs of me taken during a WORM workshop are used in WORM communication and dissemination materials.

☐ I understand that the personal data collected during the research will re-main confidential and protected in accordance with relevant data protection legislations and research integrity. The information I have provided during the research can be used as anonymized statements in the publications. My identity as an individual research participant will not be disclosed in a scientific publication or any other re-search results to be published.

☐ I agree that I can be contacted at a later stage for a further study or follow-up study.

☐ I hereby give my voluntary consent to participate in this research.

_____

The research participant's signature and name in block letters

(Consent can also be given electronically, for example, by email.)

_____

Place and date

_____

[WORM researcher's name and contact details]

Hanken School of Economics
Arkadiankatu 22, 00100 Helsinki, Finland
Postal Address: P.O.Box 479, 00101 Helsinki, Finland
Phone: +358 (0)29 431 331

Funded by the European Union

ANNEX 3 Privacy Notice

The Research's Privacy Notice

This privacy notice describes what personal data will be collected from you as a participating individual, and why and how the personal data will be processed in the research, as well as the details of the research and related participation. It also provides the information on what rights you as the data subject have pertaining to your personal data and how you can exercise these rights in relation to the processing.

Date: _12.2.2024

Working title of the research: WORM

The research is conducted for the WORM research project.

1. Data Controller

Data controllership:

Hanken School of Economics Arkadiankatu 22, 00100 Helsinki, Finland Postal Address: P.O.Box 479, 00101 Helsinki Phone: +358 (0)29 431 331 Business ID: FI02459077

Hanken's Data protection officer (DPO): dpo@hanken.fi

Questions regarding the research and personal data processing are addressed to the contact person(s): Gyöngyi Kovács, kovacs@hanken.fi

2. Information about the research

Participation in the research is not expected to cause any risk, harm or inconvenience to the research participants. No rewards will be paid for the participation in the research study.

Research data will be processed during the data analysis phase in a manner that the research participants are not directly identifiable. Direct and strong indirect identifiers such as names, addresses, and unusual job titles will be replaced with random pseudonyms, aliases or codes.

The identity of an individual research participant will not be disclosed in a scientific publication and any other research results to be published.

The research is a single study, but the research participants may be contacted later for a further study if they give their consent to such contact.

Research members who will carry out the research activities and be authorised to process the personal data during the research are: The WORM consortium

The principal investigator (PI) or person in charge of the research is: Gyöngyi Kovács

3. Purposes of processing personal data

The purpose of personal data processing is scientific research. The research will only process the personal data that are necessary and proportionate to the accomplishment of the research tasks and execution of the research.

The personal data will be processed for the research to examine: Waste in humanitarian Operations: Reduction and Minimisation (WORM)'s overall objective is designing guidelines and support actions for circular economy in the humanitarian sector. WORM focuses on two selected settings: field hospital deployments, and humanitarian livelihood programmes with a waste picking component. Across these settings, the project focuses on several cross-cutting focus areas:

- the integration of bio-based technological innovation solutions in the humanitarian context,

Funded by the European Union

- using procurement as a gatekeeper for waste avoidance, and gateway to integrate innovative solutions,
- improvements in waste management, and the use of less polluting waste treatment methods,
- a specific focus on the sustainable livelihoods of waste pickers, and
- policy development, advocacy and a heightened local awareness of improved waste management in the relevant local contexts.

[Personal data is used for the grouping to specific stakeholder groups / types of organisations.]

4 Legal bases for processing personal data

The legal basis/bases for the processing of personal data is/are:

- Processing is necessary for scientific or historical research purposes or statistical purposes, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The data subject has given consent to the processing of the personal data for one or more specific purposes. Consent is freely given and the data subject can withdraw consent at any time.

5. Categories of data subjects

The research's population of interest is: Humanitarian organisations, waste treatment organisations, hospital waste management staff, people involved in waste management, procurement experts

Estimated number of the organizations in the research: 30-50 organisations.

Estimated number of the research participants in the research: 50-200 research participants.

6. Categories of personal data

The following types of personal data will be collected and processed:

- Information which the research participant provides through a questionnaire or survey.
- Interview responses.
- Audio or video recordings and the transcribed version in a text form.
- Findings, observations or notes made by the researcher about the research participant.
- Personal data from public websites or mass media (e.g., news stories with citations from individuals).

No special categories of personal data or other specially protected personal data will be collected and processed in the research.

A Data protection impact assessment (DPIA) has been conducted by consulting Hanken's Data protection officer (DPO) prior to data collection and processing.

7. Sources of personal data

Personal data will be collected from the research participants through interviews, surveys or questionnaires.

8. Recipients of personal data

Others to whom the personal data will be disclosed:

- The research members and partners will have access to the personal data for the purpose of conducting the research.
- A third party outside Hanken who provides transcription service or data analysis service will have access to the personal data (specified below). A Data processing agreement (DPA) will be made with the party.

Funded by the European Union

The third party outside Hanken and others who will have access to the personal data are: Transcription and translation services, to be procured separately. A DPA / NDA will be part of that process.

9. Storage and security of personal data

The data controller(s) will be responsible for taking appropriate technical and organisational measures including pseudonymisation and encryption to protect the personal data against unauthorized access or illegal use and against damage to or loss of the personal data.

Contact information and other direct identifiers will be stored separately from all other data and not used for purposes non-related to this research.

Personal data in digital form will be stored and backed up securely in:

- the researcher's password-protected personal computer and hardware.
- IT systems provided by Hanken (e.g., Hanken's H: drive, OneDrive for Business, Webropol, SPSS).
- IT systems not provided by Hanken, CSC or any of the data controllers. A Data processing agreement (DPA) will be made with the service provider.

For secure data transfers, the research project will use:

- OneDrive storage space in Hanken-provided account to share files with the research partners or supervisor. "Specific people"-option will be used to ensure access control.

10. International data transfers

Data transfers between the research partners outside the EU/EEA will be restricted to anonymized data and be made via a secure channel.

11. Retention and erasure of personal data

Data retention and erasure plans: All the personal data will be erased within five years after the completion of the research project.

Data archival plans:

- The anonymised research data will be archived in a data repository such as IDA, Aila or Zenodo for later and shared reuse.

12. Data subjects' rights

According to the General Data Protection Regulation of the European Union (GDPR, EU 679/2016), you as the data subject have the right to:

- receive transparent information on the processing of your personal data and how you can exercise your rights (Art.12),
- access the personal data collected and processed (Art.15),
- have the inaccurate or incomplete personal data corrected (Art. 16),
- have your personal data erased (the right to be forgotten) in certain situations (Art. 17),
- restrict the processing of your personal data in certain situations (Art. 18),
- have your personal data transferred between systems in certain situations (Art. 20),
- object to the processing of personal data in certain situations (Art. 21),
- not be subject to automated decision-making, with certain exceptions (Art. 22), and
- be informed of a personal data breach involving a high risk (Art. 34).

When personal data processing is for archiving, scientific or historical research or statistical purposes, the rights may be restricted under the GDPR and Finnish Data Protection Act (1050/2018). Restrictions of rights always require special protective measures.

Funded by the European Union

Personal data will always be processed lawfully, fairly, and in a transparent manner to protect the fundamental rights and freedoms of the data subjects. The data controller(s) follow a GDPR-compliant procedure to respond to subject access requests.

If you have questions or requests related to data protection or the processing of personal data, you can contact the contact person(s) or Data protection officer (DPO) mentioned above.

You have the right to lodge a complaint with the supervisory authority if you feel that the processing of your personal data is an infringement of data protection laws.

Contact information of the supervisory authority/Data protection authority (DPA) in Finland:

Office of the Data Protection Ombudsman Visiting address: Lintulahdenkuja 4, 00530 Helsinki, Finland Postal address: PO Box 800, 00531 Helsinki, Finland Switchboard: tel. +358 29 566 6700 Registry: +358 29 566 6768 Email: tietosuoja@om.fi https://tietosuoja.fi

worm

Waste in humanitarian Operations:
Reduction and Minimisation

Funded by the
European Union