WinWin 4 WorkLife

D1.3 Ethics and Security Management Report

Organisation: hbits

Main author: Joeri Minnen (hbits)

Contributing authors: Veronique Van Acker, Clément Stefancic (LISER), Milad Malekzadeh (UH)

Date: 23/07/2025

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DELIVERABLE D1.3 – VERSION 1.4

WORK PACKAGE N° 1

Nature of the deliverable		
R	Document, report (excluding the periodic and final reports)	X
DEM	Demonstrator, pilot, prototype, plan designs	
DEC	Websites, patents filing, press & media actions, videos, etc.	
OTHER	Software, technical diagram, etc.	

Dissemination Level		
PU	Public, fully open, e.g. web	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Versioning and contribution history			
Version	**Date**	**Description and comments**	**Author(s)**
0.1	30.04.2024	Draft structure	Joeri Minnen (hbits)
0.2	15.05.2024	Index, gathering of information	Joeri Minnen (hbits)
0.3	30.06.2024	Initial version + discussion on progress meeting	Joeri Minnen (hbits)
0.4	30.09.2024	Creation of table structure and Ethics and Security input from partners	Joeri Minnen (hbits)
0.5	12.12.2024	Review of the document	Joeri Minnen (hbits)
0.6	20.01.2025	Inclusion of ethic documents	Joeri Minnen (hbits)
0.7	24.01.2025	Version for Internal Ethics Advisor	Joeri Minnen (hbits)
0.8	24.02.205	Comments Internal Ethics Advisor	Hans Schmeets (University of Maastricht)
0.9	28.02.205	First Cleaned version	Joeri Minnen (hbits), Hans Schmeets (University of Maastricht)
0.10	14.03.2025	Internal review version	LISER, University of Helsinki
0.11	24.03.2025	DPO LISER review	LISER + Veronique Van Acker
0.12	07.04.2025	Solving comments	Joeri Minnen (hbits)
1.0	28.04.2025	Final version for submission	Joeri Minnen (hbits)
1.1	09.07.2025	First version based on review by EC: Input about Digital Nomad Survey	Beatriz De Stefani Cardoso (IST-ID), João Abreu e Silva (IST-ID)
1.2	10.07.2025	Comments PI and hbits	Veronique Van Acker (LISER), Joeri Minnen (hbits)
1.3	18.07.2025	Second version based on comments	Beatriz De Stefani Cardoso (IST-ID), João Abreu e Silva (IST-ID)
1.4	22.07.2025	Final version for re-submission addressing comments from the review meeting	Joeri Minnen (hbits)

Acknowledgements

This report is part of the deliverables from the project “WINWIN4WORKLIFE" which has received funding from the European Union’s Horizon Europe research and innovation program under grant agreement No 101132580.

Project summary

WinWin4Worklife (WW4WL) envisions to enable healthy, inclusive and sustainable remote working arrangements (RWA) in Europe by combining employer and employee perspectives into a single framework. The project has five key objectives and outcomes:

1) To gain an interdisciplinary understanding of how the private and work spheres interact when working remotely;
2) To assess which living and working conditions ensure a healthy work-life balance in RWA for both men and women living in urban, rural, and cross-border areas;
3) To develop forecasting models of the impacts of different scenarios of RWA on mobility, land use, air quality, noise, and health;
4) To enhance knowledge on the role of culture, regional context and welfare systems in the uptake of RWA by employees and employers; and
5) To develop a comprehensive set of evidence-based spatial policies for a sustainable implementation of RWA, based on co-creation processes with stakeholders and citizens.

To do so, WinWin4WorkLife will collect novel and comprehensive data in 5 European countries (DE, FI, LU, PT, SK), selected to represent different welfare systems, housing and labour markets, and cultural norms towards remote work.

Data collection consists of an employer survey focused on organizational support for RWA, impacts on skills retention and productivity, and intentions to relocate; and an employee survey complemented by interviews and a time use app covering employee circumstances, gendered RWA experiences, impacts on work-life balance and mental health, as well as residential or job relocation, and social security and taxation issues. This quantitative and qualitative data will feed custom-made spatial forecasting models to assess wider urban/rural regeneration, environmental and health impacts.

Close and continuous engagement with planning, policy, business, and institutional stakeholders will ensure concrete and context-sensitive policy actions and measures for the sustainable uptake of RWA in Europe.

Executive summary

This document serves as Deliverable D1.3 of the WinWin4WorkLife (WW4WL) project, outlining the Ethics and Security Management Report (ESMR) for the project. The document continues deliverable D1.2, being the Data Management Plan (DMP), which has the purpose to describe how data within the WW4WL project is managed by establishing and standardizing data types, formats, storage, security measures, maintenance procedures, and alignment practices in accordance with the FAIR data principles.

The goal of the ESMR is to describe and realize the ethical and security management requirements to collect and process data during the WW4WL project. This is done by discussing the standards and methodologies to be considered for all phases of the project and throughout all relations with data and Data Subjects: from the collection of data to the valorisation of data and the sharing of data. The primary focus is on (sensitive) personal data. However, because of the WW4WL's highly critical nature of collecting and processing data every data type is part of the risk analysis. For this a Data Protection Impact Assessment (DPIA) will guide the consortium.

This deliverable functions as a guidebook for all project partners, providing structured ethical and security management procedures, methodologies, and tools to be applied during the project. Its aim is to ensure the delivery of quality-assured results and outputs while preserving the integrity of the project.

Chapter 1 introduces the context of the document, outlining the platforms used—such as SharePoint, MOTUS, and the Delphi study—and highlighting affiliated projects. Chapter 2 identifies the key contacts and their roles within the project network. Chapter 3 presents responses to the ethics self-assessment, ensuring transparency in research practices. Chapter 4 focuses on core ethical principles, including GDPR compliance, privacy by design, and oversight mechanisms. Chapter 5 categorizes the various types of data collected and used in the project, such as personal data. Chapter 6 addresses informed consent, the rights of data subjects, and the processes of anonymisation and pseudonymisation. Chapter 7 details the data security measures in place, including technical safeguards, storage protocols, and incident response strategies. Finally, Chapter 8 aligns the project with established research integrity frameworks like ALLEA and GSBPM, emphasizing respect, accountability, and transparency.

The ESMR includes several Annexes that complementary the report. These Annexes provide detailed information that supports and elaborates on the broader principles outlined.

Table of content

List of Figures

List of Tables

Abbreviations and Acronyms

Abbreviation	Description
2FA	Two-factor authentication
ALLEA	All European Academies
AP	Affiliated Project
API	Application Programming Interface
CA	Consortium Agreement
CoA	Confidentiality Agreement
DDoS	Distributed Denial-of-Service
D(L)	Deliverable
DMP	Data Management Plan
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPP	Data Protection Policy
EC	Ethics Committee
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ESMR	Ethics and Security Management Report
EA	Ethcis Application
EU	European Union
FAIR	Findability, Accessibility, Interoperability, and Reusability
GA	Grant Agreement
GDPR	General Data Protection Regulation
GSBPM	Generic Statistical Business Process Model
HTTPS	HyperText Transfer Protocol Secure
ID	Identification
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO(number)	International Organization for Standardization
ISO	Information Security Officer
JSON	JavaScript Object Notation
OECD	Organisation for Economic Co-operation and Development
OSM	OpenStreet Map
PD	Privacy Declaration
PI	Principal Investigator
POI	Point Of Interest
MOTUS	Modular Online Time Use Survey
NACE	Nomenclature of Economic Activities
NDA	Non-Disclosure Agreement
RoPA	Record of Processing Activities
RWA	Remote Working Arrangement
SSH	Social Sciences and Humanities

SSL	Secure Sockets Layer
TLS	Transport Layer Security
UNECE	United Nations Economic Commission for Europe
UI	User Interface
UX	User eXperience
WW4WL	WinWin4WorkLife
WP	Work Package

Abbreviation	Consortium Partners
DCHE	Danish Committee for Health Education
EQY	Euroquality
hbits	hbits
IST-ID	Instituto Superior Técnico
TREX	Trexima
TUM	Technische Universität München
LISER	Luxembourg Institute of Socio-Economic Research
PRO	Prolepsis
UH	University of Helsinki
UM	University of Maastricht
UNIZA	University of Žilina
UPM	Universidad Politécnica de Madrid
VUB	Vrije Universiteit Brussel
ZEW	Zentrum für Europäische Wirtschaftsforschung

Definitions

Term	Description
Anonymisation	The processing of personal data in such a way that individuals cannot be identified from it, ensuring privacy and confidentiality.
Anonymised data	Data that have had personal identifying information removed so that the individuals or entities represented in the data cannot be re-identified.
Collected data	Data that have been collected by the user.
Data Controller	A legal or natural person, an agency, a public authority, or any other body who determines the purposes for which and means by which personal data is processed.
Data Manager	An individual tasked with coordinating and supervising the collection, storage, and utilisation of project-related data, ensuring it aligns with project objectives and complies with relevant regulations.
Data Processor	A legal or natural person, an agency, a public authority, or any other body who processes personal data on behalf of the Data Controller, following their instructions and guidelines.
Data Protection Impact Assessment (DPIA)	A DPIA describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible.
Data Protection Officer (DPO)	A designated individual within an organisation who oversees data protection and ensures compliance with data protection laws and regulations.
Data Sharing Agreement	A formal document that defines the terms and conditions under which personal data is transferred between entities, ensuring compliance with data protection conditions.
Data Storage	The process of encoding and preserving digital information on physical media for future retrieval, encompassing various devices and technologies like hard drives, SSDs, and cloud storage.
Data Subject	An individual whose personal data is collected, processed, or stored by an organisation.
Detected Data	Information automatically captured or generated by sensors, devices, or systems, often in real-time, as a result of monitoring activities or environmental conditions.
Ethics Management	Involves applying ethical principles and standards to organisational decision-making, ensuring actions, policies, and procedures reflect a commitment to ethical behaviour and the well-being of all stakeholders.
Gender Equality	All genders, regardless of their differences have the same rights, responsibilities, and opportunities, ensuring that everyone can fully participate in all aspects of life without discrimination based on gender.
Generated data	Refers to information produced through computational processes, simulations, or algorithms, often derived from existing data sets or models.

Joint Controller	Data controllers can determine the purpose and means of data processing individually or jointly with another party as joint data controllers. Joint controllers have a shared purpose and means of processing data together. However, this will not apply if the same data is being used for different reasons.
Metadata	Data that provides information about other data, describing attributes such as its format, structure, location, and usage.
Original data	These are the original data file as collected by the user or as received after a data request.
Personal data	Personal data is any information that relates to an identified or identifiable living individual ('data subject'). Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Examples are a name and surname, a home address, an email address such as name.surname@company.com, an identification card number, location data (for example location data function on a mobile phone), an Internet Protocol (IP) address, a cookie ID, the advertising identifier of your phone. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.
Primary data	Original data collected firsthand by a researcher or organisation for a specific purpose or study (in this case the WinWin4WorkLife project).
Processed data	Processed data refers to raw data that has been organized, cleaned, transformed, or analysed to make it meaningful or usable.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. This means that the use of 'additional information' can lead to the identification of the individuals, which is why pseudonymous personal data is still personal data.
Pseudonymised data	Data that have had personal identifying information replaced with a pseudonym, or id, which can be used to track and manage the data without revealing the identity of the individuals or entities it represents.
Research data	Refers to factual records, measurements, observations, or other findings obtained through systematic investigation and used as a basis for analysis, interpretation, or publication in research activities.

Research Integrity	The ethical and responsible conduct of research, encompassing honesty, rigor, transparency, and accountability throughout the entire research lifecycle, from initial idea to publication.
Secondary data	Data that has been previously collected and processed by others, often for different purposes, and is used for analysis or research by a new user.
Security management	The identification of an organisation's assets i.e. including people, buildings, machines, systems and information, followed by the development, documentation, and implementation of policies and procedures for protecting assets.
Stored data	The information that has been recorded and preserved in a digital format.
Working data	These are the data files that have been derived from the original data to be used for analytical purposes. Working data are not necessarily equal to the original data.

1. Introduction

1.1. Context of this document

The purpose of the ESMR is to ensure that project activities are conducted responsibly, honestly, transparently, and safe. This document has been formulated based on various standards on the European, international and national level, but also gathered information on the institutional level. In this way the deliverable and the practicalities within the WW4WL project lead to protocols or guidelines that balance to a comprehensive overview of the ethics and security guidelines, legal considerations, and standards, laying out a general framework for WW4WL partners to be followed throughout the project's duration, and if applicable also after the project.

An important focus goes to the research activities that belong to the core of the WW4WL project. Central to the actions of WW4WL stands the participation of employers and employees (both seen as respondents) to studies to collect information, and the involvement of stakeholders during interactive moments, both to get insights on the topic of Remote Working Arrangements (RWA). These interactions have their specific goals, recruitment methods, efforts to ensure representativeness, inclusivity, and equality, and methodologies to collect and gather the needed data.

In more detail, the ESMR presents the actions and measures the consortium will implement to ensure compliance with the framework, responsible research practices, security, and scientific integrity. These also include essential tools, like informed consent procedures and forms, research integrity compliance, ethics approvals, and the establishment of management structures for ongoing ethics monitoring. The document has an important focus on the collection of (sensitive) personal data, along with corresponding protection needs and procedures, such as data minimization, anonymisation, pseudonymisation, and organizational and technical safeguards. Moreover, this document also establishes and disseminates a basic set of guidelines for internal communication.

This ESMR is actively updated throughout the project's duration, with continuous monitoring of issues and documentation of new concerns as they (might) arise for future reporting.

hbits and LISER have collaborated to compile a check list of ethical and security considerations (ANNEX 1) in support of the content of this report. This list has been distributed to the consortium partners, who will diligently oversee and manage the procedures outlined in these documents under the supervision of the project's Project Board and the External Ethics Committee.

The External Ethics Committee is composed of three members:

- Sona Ftacnikova (Slovak Centre of Scientific and Technical Information)

- Frank Cövers (University of Maastricht)
- Rémi Suchon (Catholic University of Lille)

1.2. Platforms for WW4WL

To support the activities for WW4WL the consortium makes use of an own developed website for external communication and participation with important groups to the project, of a SharePoint portal for internal communication and coordination, of the MOTUS data collection platform for the collection and storing of data during data phases of data collection, and of a Delphi survey platform for gathering information from stakeholders.

1.2.1. Website WW4WL

The WW4WL website is both an important source of (providing) information, as well as an entrance for employers, employees and stakeholders to take part to the project. Therefore, the website is the first medium to come in touch with the project and therefore the portal to explain and show what the goals of the WW4WL project are and how Ethics, Security and Research Integrity are considered.

The website can be consulted by the following url: https://winwin4worklife.eu.

1.2.2. SharePoint platform

Microsoft SharePoint serves as the online collaboration platform for the WinWin4WorkLife project, overseen by EQY. A dedicated project site has been created on this platform, accessible exclusively to partner representatives within the consortium.

This SharePoint site will be used for storing project deliverables and facilitating collaborative work on publications and reports.

1.2.3. MOTUS data collection platform

The development of the MOTUS data collection platform started in 2012 as an academic project of the Vrije Universiteit Brussel (Belgium). To further improve and scale up the development of the platform the spin-off hbits CV was established in 2018. From that point onwards hbits CV is further developing and commercialising the platform. The platform is mainly used for academic projects and by National Statistical Institutes.

The use of one and the same data collection platform for the collection of data from employers and employees is seen as a main asset for the WW4WL project.

In the WW4WL project and through MOTUS multiple data collection methods are employed. Surveys will be taken from employers and employees; a time diary will be kept by employees while they will also respond to extra questions; and employees will be asked for consent to be geotracked over a period of at maximum two weeks. All

actions from providing contact information to the collection of data is arranged via the MOTUS platform. Automized procedures and study related communication are defined via the platform. The platform is hosted on ISO27001 servers.

To ensure privacy and security of data, data collections are done under control of the case study leaders, their respective institutions (Ethical Committees and DPO), and their respective Data Managers. The WW4WL project has the availability over an own Namespace 'WW4WL'. Every case study leader has the availability over a separate Group within the platform to organise their data collection in a privacy and secure manner (ANNEX 2).

Error! Reference source not found. illustrates the platform architecture of MOTUS.

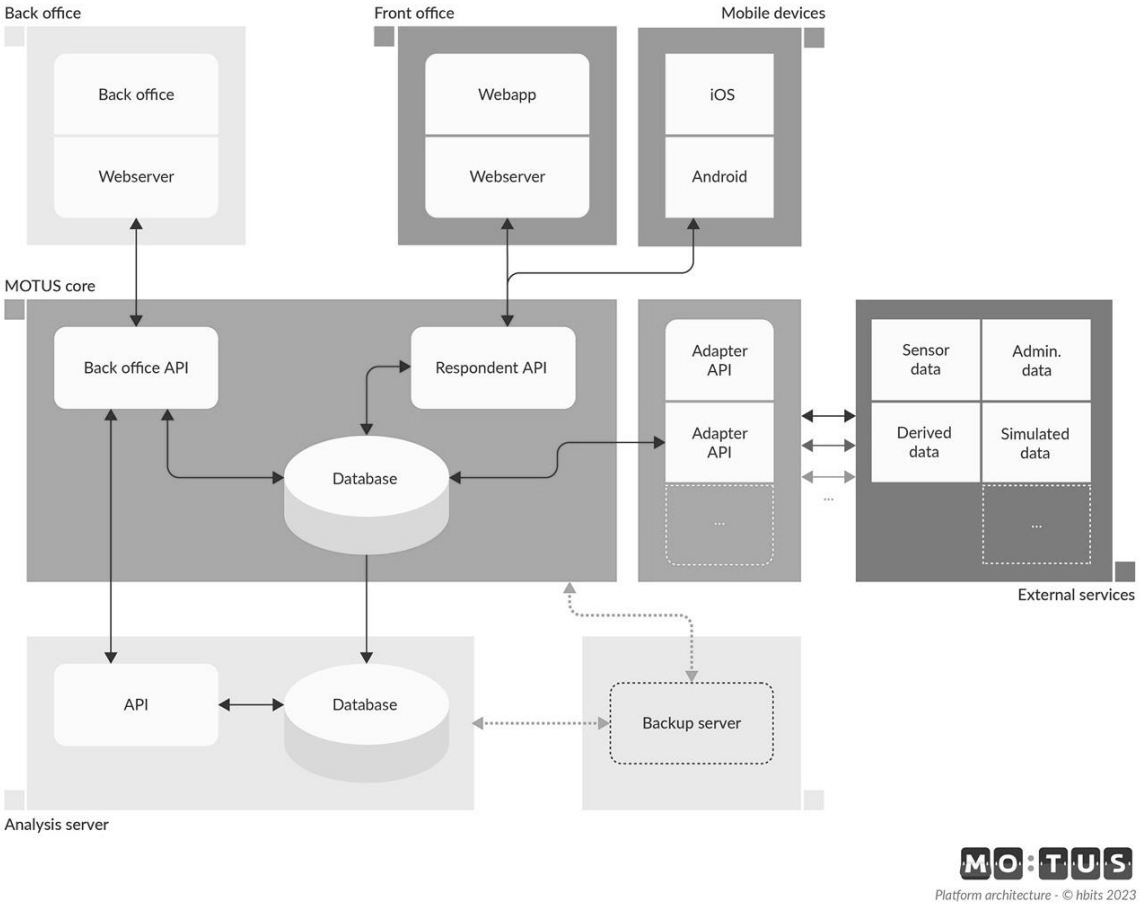

Figure 1: Platform architecture MOTUS

The MOTUS data collection platform consists of a front office and a back office.

The front office is the collection tool or application with which users interact via a user interface (UI), delivering a user experience (UX). The MOTUS application is available as a web version for browsers (https://app.winwin4worklife.eu) and as iOS and Android mobile versions for smartphones and tablets. The application is designed to simplify

the process for respondents to complete tasks in various surveys, such as time use surveys.

The back office is responsible for building studies, facilitating data collection and monitoring, and processing data. It is accessible via a web environment and contains several builders. Both the front office and back office connect to the MOTUS core ("the core") through Application Programming Interfaces (APIs). The core hosts the database with all information needed to build studies and collect data. A separate analysis server holds a replica of the core database and supports information processing in the back office. The back-up server is a replica of both the core and the analysis server.

Adapter APIs enable the adaptation of external information for processing in the core, allowing the ingestion of passive data from integrated sensors or connected devices, administrative or secondary data from external sources, or other processed data. For optimization, data security, and privacy, these data are managed and organized in an anonymised manner within stand-alone microservices. All user input is encrypted and sent to the server via HTTPS communication and is immediately synchronized across all of the user's devices via the respondent API. Consequently, the MOTUS web and mobile applications can be used interchangeably.

MOTUS is deployed as a cloud-based infrastructure. In this approach, all MOTUS components (such as the core and back office) and microservices run in their own containers. This containerized environment offers better scalability, enhanced application monitoring, and decoupling from the underlying infrastructure.

1.2.4. KoboToolbox data collection platform

In addition to the employer and employee surveys in MOTUS, digital nomads will also be surveyed about their experiences. This task is carried out by IST-ID where they use the KoboToolbox data collection platform for this digital nomad survey.

The development of the KoboToolbox data collection platform began in 2005 as an initiative of the Harvard Humanitarian Initiative (United States), with the goal of supporting data collection in challenging environments, particularly in humanitarian crises and low-resource settings. Since then, KoboToolbox has evolved significantly, with continuous contributions from the global humanitarian, academic, and development communities. Today, KoboToolbox is maintained and further developed by the Harvard Humanitarian Initiative with support from various partners and donors. The platform is widely used by UN agencies, NGOs, research institutions, and governments (KoboToolbox, 2025a).

A key advantage of KoboToolbox in many projects is its ability to provide a single, flexible data collection platform for gathering information from a wide variety of sources, including community members, field staff, and partner organizations. For example, in humanitarian response programs, KoboToolbox enables teams to collect

needs assessments, monitoring data, and feedback from affected populations through standardized and customizable tools (KoboToolbox, 2025b).

KoboToolbox supports multiple data collection methods within a single platform; surveys can be conducted offline or online using mobile devices such as smartphones and tablets, or through web forms on computers. The platform allows for complex questionnaires, skip logic, multimedia integration (such as photos, audio, and GPS), and form version control. Data collection, from the initial survey design to data submission, is fully managed via KoboToolbox. The platform also supports automated data validation rules and study-specific communication workflows. Data is hosted on secure servers that comply with international standards for information security (KoboToolbox, 2025c).

To protect privacy and ensure data security, data collection activities are carried out under the supervision of the implementing organization's ethical boards, data protection officers, and data managers. KoboToolbox allows organizations to create separate projects and user groups, facilitating secure and organized data management for different teams and studies. It is possible to use the main server (based in United States), or opt for the server located in the European Union, which is hosted in Ireland. This server is used by organizations that require or prefer data to be hosted in the European Union and that respect GDPR legislation. Besides that, the data from both servers is stored on Amazon Web Services (AWS) servers (KoboToolbox, 2025d).

KoboToolbox utilizes ISO 27001 compliant facilities for its servers and implements other security measures such as encryption both in transit and at rest. Additionally, KoboToolbox has data security policies and audits in place, and also offers Data Processing Agreements for GDPR compliance (KoboToolbox, 2025d). A positive point about the platform is that it is not necessary to create an account to access its questionnaires (as a respondent), and the IP address of the data collected is not accessible without formal authorization from the platform and the hosted server, which reinforces the anonymity and protects the identity and location's information of the answers obtained.

The KoboToolbox data collection platform consists of two main components: the data collection interface (front end) and the management and processing environment (back end). The front end includes the tools with which users interact to complete forms, whether via the KoboCollect mobile app (available for Android) or through the web-based Enketo forms accessible on browsers. These tools are designed to make data collection intuitive and efficient, even in remote areas with limited connectivity. Responses can be saved locally and submitted when an internet connection becomes available (KoboToolbox, 2025c).

The back end consists of the project management console, where users design forms, manage projects, monitor incoming data, and export datasets. The platform architecture is API-driven, with the core database securely storing all collected data. The system supports real-time synchronization of data between devices and the server

when connectivity allows. KoboToolbox also offers integration options via APIs for connecting with external systems or importing secondary data (KoboToolbox, 2025c).

KoboToolbox is deployed as a cloud-based solution with the option for organizations to self-host for greater control over data sovereignty and security. Its scalable infrastructure enables teams of all sizes to deploy data collection projects efficiently and securely.

1.2.5. Delphi survey platform

Stakeholders will take part to a Delphi study balancing their own views with the views of other stakeholders.

This task is carried out by UPM and will start later in the project. Information on the platform used, and the technicalities are described in a later version of the ESMR.

1.3. Affiliated projects

The WW4WL has Affiliated Projects (AP). On the website a dedicated section (https://winwin4worklife.eu/about/related-projects/) is present where the different projects are showcased aligned to their mission in enhancing the understanding of RWAs and the promoting of a better work-life balance. Through collaboration and knowledge-sharing WW4WL amplifies the impact of research integrity to share our goals, insights and learning. The website provides the opportunity to explore each contributing valuable insights and solutions to the evolving landscape of remote work.

Each AP adheres to rigorous ethical guidelines and implements robust security measures to protect sensitive information. Explore the individual ethic and security policies of each project to learn more about their commitment to maintaining integrity, confidentiality, and compliance with regulations.

2. Contact overview

A contact overview plays a pivotal role in ensuring compliance with data protection regulations, managing privacy risks, fostering transparency and accountability, and enhancing overall data governance practices within a project like the WW4WL project.

Below two tables are compiled, a first table from the viewpoint of specific roles within the WW4WL project with a particular focus on data collection, and a second table which lists all legal positions that are encountered within the WW4WL project.

Table 1: Overall contact points

Roles project level	Person - Institution	Contact e-mail
Principal Investigator	Veronique Van Acker - LISER	veronique.vanacker@liser.eu
Project level Data Manager	Marián Magdolen - UNIZA	marian.magdolen@uniza.sk
Internal Ethics Advisor	Hans Schmeets - UM	h.schmeets@maastrichtuniversity.nl
WP3 leader – Data collections	Yannick Cornet - UNIZA	yannick.cornet@uniza.sk
Case study 1 Data Manager - Employer and Employee study - Luxemburg	Marc Schneider - LISER	marc.schneider@liser.lu
Case study 2 Data Manager - Employer study - Germany	Daniel Erdsiek - ZEW	Daniel.Erdsiek@zew.de
Case study 3 Data Manager – Employee study - Germany	Ana Moreno - TUM	ana.moreno@tum.de
Case study 4 Data Manager – Employer and Employee study - Finland	Olle Järv - UH	olle.jarv@helsinki.fi
Case study 5 Data Manager – Employer study - Slovakia	Michal Hrnčiar - TREX	hrnciar@trexima.sk
Case study 6 Data Manager – Employee study - Slovakia	Eva Malichová - UNIZA	eva.malichova@uniza.sk
Case study 7 Data Manager – Employer and Employee study - Portugal	João de Abreu e Silva – IST-ID	jabreu@tecnico.ulisboa.pt
WP7 leader – Interview and Delphi study	Julio A. Soria-Lara - UPM	julio.soria-lara@upm.es
Data collection platform MOTUS	Joeri Minnen - hbits	Joeri.Minnen@hbits.io
Data collection platform KoboToolbox	João de Abreu e Silva - IST-ID	jabreu@tecnico.ulisboa.pt
Project and social communication	Antonia Nikolova - EQY	antonia.nikolova@euroquality.fr

Table 2: Legal positions per consortium member

Member	Legal position	Name	Contact e-mail
LISER	Principal Investigator	Veronique Van Acker	veronique.vanacker@liser.lu
	Data Manager	Marc Scheider (data sharing) Anasse El Maslohi (data cleaning & management)	Marc.schneider@liser.lu Anasse.ElMoslohi@liser.lu
	DPO	Clément Stefancic	Clement@luxgap.com
	Legal department	Elise D'Errico Clément Stefancic	Elise.Derrico@liser.lu Clement@luxgap.com
EQY	Principal Investigator	Antonia Nikolova	Antonia.nikolova@euroquality.fr
	Data Manager	Yannick Lafon	Yannick.lafon@euroquality.fr
	DPO	Yannick Lafon	Yannick.lafon@euroquality.fr
	Legal department	Doris Monjac	Doris.monjac@euroquality.fr
VUB	Principal Investigator	Theun Pieter van Tienoven	Theun-Pieter.van.Tienoven@vub.be
	Data Manager	Johan Surkyn	Johan.Surkyn@vub.be
	DPO	Andries Hofkens	andries.hofkens@vub.be
	Legal department	-	LEO@vub.be
hbits	Principal Investigator	Joeri Minnen	Joeri.Minnen@hbits.io
	Data Manager	Joeri Minnen	Joeri.Minnen@hbits.io
	DPO	Joost Roelens	dpo@hbits.io
	Legal department	Joost Roelens	dpo@hbits.io
PRO	Principal Investigator	Dimitrios Linos	Dlinos@hms.harvard.edu
	Data Manager	Dimitra Pinotsi	d.pinotsi@prolepsis.gr
	DPO	Panoraia Spilopoulou	panoraia@gmail.com
	Legal department	Panoraia Spilopoulou	panoraia@gmail.com
DCHE	Principal Investigator	Charan Nelander	cn@sundkom.dk
	Data Manager	Andreas Jespersen	aj@sundkom.dk
	DPO	Mette Laub Pedersen	mlp@sundkom.dk
	Legal department	Charan Nelander	cn@sundkom.dk
IST-ID	Principal Investigator	João de Abreu e Silva	jabreu@tecnico.ulisboa.pt
	Data Manager	João de Abreu e Silva	jabreu@tecnico.ulisboa.pt
	DPO	Fatima Ferreira	dpo@ist-id.pt
	Legal department	Cláudia Figueira	Apoio.juridico@tecnico.ulisboa.pt
TUM	Principal Investigator	Ana Moreno	ana.moreno@tum.de
	Data Manager	Ana Moreno	ana.moreno@tum.de
	DPO	Uwe Baumgarten	baumgaru@tum.de
	Legal department	Franziska Schiffner	franziska.schiffner@tum.de
ZEW	Principal Investigator	Daniel Erdsiek	Daniel.Erdsiek@zew.de
	Data Manager	Daniel Erdsiek	Daniel.erdsiek@zew.de
	DPO	Thomas Wirth	thomas.wirth@zew.de
	Legal department	Thomas Wirth	thomas.wirth@zew.de
UMP	Principal Investigator	Julio A. Soria-Lara	julio.soria-lara@upm.es
	Data Manager	Amor Ariza-Álvarez	mariaamor.ariza@upm.es
	DPO	Luis Cancela de la Viuda	proteccion.datos@upm.es

	Legal department	Elena Martinez Nieto	elena.martinez@upm.es
UNIZA	Principal Investigator	Tatiana Kovacikova	tatiana.kovacikova@uniza.sk
	Data Manager	Eva Malichová	eva.malichova@fri.uniza.sk
	DPO	Marián Magdolen	marian.magdolen@uniza.sk
	Legal department	Janka Stanikova	janka.sanikova@uniza.sk
UH	Principal Investigator	Olle Järv	olle.jarv@helsinki.fi
	Data Manager	Olle Järv	olle.jarv@helsinki.fi
	DPO	UH DPO	tietosuoja@helsinki.fi
	Legal department	UH Legal Counsel	tutkimuksenjuristit@helsinki.fi
UM	Principal Investigator	Pim Mertens	Pim.mertens@maastrichtuniversity.nl
	Data Manager	Fieke Wouters	Fieke.wouters@maastrichtuniversity.nl
	DPO	Raoul Winkens	fg@maastrichtuniversity.nl
	Legal department	Legal Affairs	secretariaat-jz@maastrichtuniversity.nl
TREX	Principal Investigator	Michal Hrnčiar	hrnciar@trexima.sk
	Data Manager	Michal Hrnčiar	hrnciar@trexima.sk
	DPO	Frantisek Foltán	foltan@trexima.sk
	Legal department		

All together these roles should result in the compliance with the regulations, should execute and evaluate risk management, should protect the principle of data minimization, should take care for transparency and accountability, should be in first line organize response to Data Subject requests, should propagate incident response and reporting and should establish a clear and robust data governance practise.

These overall responsibilities and tasks are in more detail discussed in the underlying document.

3. Answers to the Ethics Self-Assessment

The ESMR draws knowledge and requirements from various sources including the project's Grant Agreement (GA), the applicable international, EU and national laws, scientific integrity guidelines, human rights principles, data protection principles, and research ethics standards. It primarily focuses on the conduct and practices of consortium partners in the collection of research data that involves personal and sensitive data from Data Subjects and from stakeholders, as well as the related processing, valorisation and dissemination of personal and sensitive data and the outcomes of the research activities.

To identify and deal correctly with any ethics issues and to adhere to underlying laws and frameworks the WW4WL projects completed the Ethics Self-Assessment guidance of the European Commission.

Most importantly, actions within WW4WL relate to the following practices:

- **work with human participants**, i.e. research or study participants, that are either employers or employees to complete questionnaires, diaries, or are geotracked, or members to a stakeholder panel partaking to interview rounds. Altogether personal and sensitive data are being collected and processed through the entire projects' duration,
- **collection and processing of personal data**, that relate to an identified, or identifiable natural person of which these personal data are processed either manually or by automatic means.

As described within the General Data Protection Regulation (GDPR)[1], (sensitive) personal data need to be gathered and handled according to principles and conditions designed to minimize impact on the individuals involved while ensuring data quality and confidentiality.

WW4WL shows alignment to the related frameworks by the development of study protocols (see 4.2 Privacy by design through Study protocols). Study protocols demonstrate the awareness of the ethical issues that are part of the methodology of the WW4WL study setup. These protocols form the basis for ethical approvals and, so, are an important tool to protect the privacy of Data Subjects, the security of the data, as well as, to protect the research integrity of researchers, and organisations in support of these researchers.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR') (OJ L 119, 4.5.2016, p. 1) (Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1797-1-1)

Throughout the ESMR, the study protocols will form the Red Thread, and follows from the Implementation plan for data collection (D3.2). ANNEX 3 will provide the template of the Study protocol to be completed by the Data Managers of the Case studies.

4. Ethical principles and research

The underlying ESMR outlines the framework of ethical, security and integrity guidelines and standards governing the WW4WL project. All aspects together are guided by Research Principles documented in the European Code of Conduct as published by ALLEA[2]. This code describes that good research practices of individual researchers, institutions, and organisations are bound to the principles "of:

- **Reliability** in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources,
- **Honesty** in developing, undertaking, reviewing, reporting, and communicating research in a transparent, fair and unbiased way,
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment,
- **Accountability** for the research from idea to publication, for its management and organisation, for training, supervision, and mentoring, and for its wider impacts"[3].

These ethical principles need to be taken into account from designing the study, over the implementation and execution of the research actions, until the dissemination of the research outcomes.

The following parts provide more detail on the crossroad of ethical principles and conducting research.

4.1. Trustworthiness, self-regulation and proportionality

The Code serves as the primary document outlining research integrity standards for all EU-funded research initiatives. The European Commission provides the research community with a framework for self-regulation. This self-regulation describes professional, legal, ethical and intellectual responsibilities, but also explains how to deal with challenges.

With these Research Principles at hand, the goal is to create trustworthiness of the research system, to define criteria for ethical research conduct, to maximize research quality and reliability, and to appropriately address threats to, or breaches of, research integrity. The checklist defined under ANNEX 1 takes up these outlined aspects for the researchers to be informed about the standards as described in the code.

---

[2] ALLEA (2023). The European Code of Conduct for Research Integrity (Revised Edition 2023). Available at: https://allea.org/code-of-conduct/

[3] Annex 5 of the Grant Agreement

Research findings have a broad display, going from datasets, metadata, publications, protocols, code, software, images and artefacts to other materials and methodologies pertinent to the research. Research Principles are also attentive to the various roles playing an essential part within the research community, bridging the aims and visions of all stakeholders. These stakeholders are not limited to individual researchers and their respective organisations but also include e.g. organisations providing research funding, performing assessment, developing policy or publishing research, and the related staff like project managers or reviewers and editors.

Research Principles undergo changes. Each new version of the Code of Conduct adapts to changes related to social, political, or technological developments as they affect the research environment. Updated Research Principles deal with new ways of interaction and communication through social media; other changes reflect how to adapt to the development and application of new technologies in the way research is conducted.

All together are persons conducting research tasks expected to respect to an ethical mindset involving good research practices, promoting openness, reproducibility, and traceability whenever feasible, and abstaining from actions that violate research integrity as outlined in the Code.

Whereas the protection of personal and sensitive information was already a key requirement, the new version of the Code of Conduct sharpens the principles towards data management practices, data protection and security (General Data Protection Regulation – GDPR), whereas also the research culture undergoes changes providing more control to the Data Subject. In a self-regulative environment, appropriate actions are defined in guidelines that incline local, national, and discipline-specific necessities. An important check-and-balance is setting appropriate actions proportional to the research goals defined in the research proposal and study protocol(s).

The WW4WL consortium commits itself to establish a culture of Research Integrity by defining specific policies and guidelines wrapped in tools and procedures that apply to the highly sensitive actions within the project related to the new research practices, and concerns, in citizen science and participatory research. The specific policies and guidelines are adapted to the WW4WL research activities, and place high value to teams co-supporting each other in conduction good research.

4.2. Privacy by design through study protocols

A study protocol serves as a blueprint for conducting a study, outlining the objectives, methods, and procedures to be followed throughout the research actions. It provides a structured framework that ensures the systematic collection and analysis of data to address specific research questions or hypotheses. By delineating the goals and parameters of the study, a research protocol not only guides the researchers in their tasks but also ensures transparency, reproducibility, and ethical integrity in the research process.

Moreover, by going through and answering a set of basic questions for the uptake of the research actions, as a researcher, it is more ensured no unexpected problems turn up at the start of the research, in gathering and processing of (sensitive) personal data from Data Subjects, and in the security and provision of various data types to other partners in the project. Possible issues could ultimately lead to being unable to conduct the research due to non-compliance with the GDPR (such as being unable to publish your research or having to delete your data).

The WW4WL project focuses on gathering innovative and comprehensive data across five European countries, involving employers and employees and stakeholders in relation to these employers and employees. This means that the design of the research components, the composition of (a) research flow(s), the collection of the data, the preparation of the datasets, the analysis of the data and the dissemination of the data are highly critical on ethics and so on privacy and security of (sensitive) personal data.

Participants engage in extended participation periods, utilizing questionnaires, time diaries, and geotracking. Privacy and security considerations are paramount, requiring a design that prioritizes privacy both by design and by default. Following data collection, anonymisation or pseudonymisation is necessary before analysis begins. Additionally, forecasting activities will be conducted, and stakeholders partake in a multi-round Delphi-approach.

A study protocol provides a guideline from designing the study, in doing the study until the processing and dissemination of the results. A template for defining a study protocol is available as ANNEX 3. The completion of this template will provide the tools and procedures that lead the WW4WL to entail privacy and security, by design and by default, in protection of Data Subjects, researchers and related institutions.

All beneficiaries within the WW4WL project must respect the outlined procedures to ensure that all research tasks have been conducted carefully and responsibly. Ethical research not only means following the correct procedures but also requires reporting on the research work done. When research work lacks on sound scientific conduct, investigation and repair actions are to be defined and implemented.

The most important research activities, research components and contexts within the WW4WL project are described in the Data Management Plan (D1.2) as well as in the Implementation Plan for Data Collection (D3.2) and relate to a specific Chapter:

- The employer survey, see Chapter 2.
- The employee survey, see Chapter 3.
- The digital nomad survey, see Chapter 4.
- The stakeholder panel, see Chapter (to be added later).

4.3. Important reflections from the GDPR, and reasons to comply with GDPR

Although the basic principles of the privacy legislation remain, updated interpretations to the GDPR brings along some important changes and obligations. As these are:

- Researchers must report (sensitive) personal data processing in a Record of Processing Activities (RoPA) ('self-accountability obligation').
- Institutions must appoint a Data Protection Officer (DPO) when processing a lot of data.
- A Data Protection Impact Assessment (DPIA) must be carried out for processing with high risk (e.g., processing sensitive data, profiling, systematic monitoring, combining datasets, using new technologies, etc.).
- Data security needs to entail encryption, anonymisation or, if anonymisation prevents achieving the processing purposes, pseudonymisation.
- Informed consent needs to comply with (the) general standards, including the newer and stricter edition (see below).
- All relevant information required by GDPR transparency obligations, including identity of the data controller, purposes and legal basis for processing, categories of data processed, recipients, retention periods, data subject rights, and any transfers outside the EU, must be clearly communicated to data subjects.
- (Sensitive) personal data breaches likely to result in a high risk to the rights and freedom of Data Subjects must be reported mandatory to the Data Protection Authority (DPA) within 72 hours.
- Transferring of (sensitive) personal outside of the European Economic Area (EEA) needs to comply to the updated rules.
- The Data Protection Authority has the authority to conduct inspections and impose fines. These fines may include both administrative fines and (personal) criminal sanctions.
- Expand the rights of Data Subjects to "the right to access" and, under certain conditions, "the right to be forgotten" and the right to data portability.

Meeting the new requirements for research is important for several reasons:

- Proper and ethical handling of data can increase the trust of citizens and Data Subjects in science.
- Research guided by the principle 'privacy by design' and 'privacy by default' better ensure the protection of (sensitive) personal data of Data subjects.
- Careful and ethical handling of data enhances the quality and reliability of the research and its results.
- Violation of the law can lead to reputational damage and negative media attention for the institution, involved researchers, and the academic community as a whole.
- Compliance with GDPR is respecting those who fund the research actions.
- When submitting publications, journals increasingly inquire about compliance with GDPR.

- Properly collected primary data also provide legal certainty to use them as secondary data in further analyses. Data processed in violation of GDPR may be unlawful and therefore must be deleted.

4.4. Monitoring ethical research

WW4WL works as a consortium in support, and positive criticism. To support researchers in good research behaviour, different levels of monitoring apply.

4.4.1.Institutional level – detailed monitoring

The most important level is the institutional level as indicated in the important notice section of the Ethics Self-Assessment guide of the European Commission. This level at first is responsible for following legal grounds in the collection and processing of (sensitive) personal data, as well as to all research actions that come across in the fulfilment of the WW4WL project.

Providing support and advise to researchers

It was already presented that institutions are required to define study protocols. Furthermore, institutions are required to provide assistance to the researcher in performing their research activities. Support and advise is received by the researcher within every university or research organisation from:

- Specialised ethics departments
- Principal Investigators
- Data Managers
- Ethics advisers

Providing ethical approval

The researcher, the different roles (PI, Data Manager, …) and the institutional experts (DPO, legal …) are responsible for meeting the ethical standards and the legal and ethical requirements on a national and international level, and to submit their application prior to the research activities to the Ethical Committee to assess SSH research within their institution. Prior to commencing any action task that raises ethical concerns, the WW4WL partners must ensure they have acquired all necessary approvals or documents required for carrying out the task.

An ethical committee provides advise not only on how (sensitive) personal data of Data Subjects need to be protected, and how privacy issues should be solved in a comprehensive manner, but also on how Data Subjects should be selected, should be contacted and should be informed. Within the WW4WL project obtaining an approval is required. Activities that raise ethical concerns must commit to additional requirements stipulated by these committees.

The following table provides an overview of the different Ethical Committees for SSH research within the WW4WL consortium.

Table 3: Institutional Ethics Committees and request for DPIA per type of responsibility

Member	Data collection and/or valorisation	Ethics board	Status application	DPIA
LISER	Data collection employers	LISER has an ethics board to apply for approval from for SSH research	Approved	Yes
	Data collection employees		Approved	Yes
	Data valorisation			Joint DPIA in preparation
EQY	Not applicable		/	/
VUB	Data valorisation	VUB has an ethics board to apply for approval from for SSH research		Joint DPIA in preparation
hbits	Not applicable	• 3 tier architecture via containerization • MOTUS privacy declaration • MOTUS as a tool for third party usage • Penetration test, Load and Performance test • ISO27001 certification • DPIA approval from LISER DPO • Platform and Role Management • Updated software platform (Laravel 11 – with security fixes until March 12th 2026) • Infrastructural support to the Rights of the Data Subjects As provider of the MOTUS data collection platform hbits is evaluated as a data processor, and therefore is part of the applications to the different institutional ethics boards that run the case studies.	/	Yes, together with each of the data controllers if deemed necessary
PRO	Data valorisation	PRO has an ethics board to apply for approval from health research	Approved, prior to DPIA	Joint DPIA in preparation
DCHE	Data valorisation	No institutional ethics board available		Joint DPIA in preparation
IST-ID	Data collection employers	IST-ID has an ethics board to apply for approval from for SSH research IST-ID is data collector for the digital nomads survey, carried out via KoboToolbox: • KoboToolbox and IST-ID have a privacy notice	Approved	DPIA requested (in bulk to the other surveys), but not necessary
	Data collection employees		Requested	DPIA requested
	Data collection digital nomads		Approved	DPIA requested

	Data valorisation	• KoboToolbox servers used for hosting to the survey • Data Processor Agreement between IST-ID and KoboToolbox • DPIA delivered by IST-ID DPO		Joint DPIA in preparation for employer and employee study; DPIA requested for digital nomad survey
TUM	Data collection employees	TUM has an ethics board to apply for approval from for SSH research	Requested	Yes
	Data valorisation			Joint DPIA in preparation
ZEW	Data collection employers	ZEW has an ethics board to apply for approval from for SSH research	Approved	Not necessary
	Data valorisation			Joint DPIA in preparation
UPM	Data collection Delphi study	UMP has an ethics board to apply for approval from for SSH research	Approved	Yes
	Data valorisation			Joint DPIA in preparation
UNIZA	Data collection employees	UNIZA does not have an ethics board to apply for approval for SSH research (Data collection and data analysis); but relates on external experts hired by UNIZA.	Requested	Yes
	Data valorisation			Joint DPIA in preparation
UH	Data collection employers	UH has an ethics board to apply for approval from for SSH research	Not necessary	Not necessary
	Data collection employees		Requested	(no info)
	Data valorisation			Joint DPIA in preparation
UM	Data valorisation	UM has an ethics board to apply for approval from for SSH research		Joint DPIA in preparation
TREX	Data collection employers	TREX does not have an ethics board to apply for approval for SSH research (Data collection and data analysis); but relates on external experts hired by TREX.	Approved	Not necessary

All documents are maintained on record via SharePoint and are available for inspection upon request by the coordinator to the granting authority. If the documents are not in English, they are accompanied by an English summary. This summary should outline how the documents pertain to the specific action tasks at hand and include any conclusions drawn by the respective committee or authority, if applicable.

Within WW4WL members of the consortium may face a different ethics board scenario. Some partners lack boards from which approvals or opinions can be sought. However, certain partners possess internal advisors who can provide guidance on ethical queries when necessary.

In the absence of a board, it remains good practice to:

• step 1; consult with an external ethics expert

• step 2; in these consultations, refer to ethical approvals other partners received from their institutional ethics board

Confidentiality

Furthermore, the consortium acknowledges its responsibilities pertaining to the general obligation to uphold confidentiality[4].

4.4.2. Project level – overall monitoring

WW4WL has an Internal Ethics Advisor in the person of Hans Schmeets serves as the Internal Ethics Advisor for WW4WL. He will address ethics issues as they arise and may consult the External Ethics Committee when necessary.

Continuous monitoring of research ethics will occur throughout the project, including oversight of consent processes and maintenance of valid ethics approvals.

The Principal Investigator, the internal Ethics Advisor together with the Data Managers will regularly attend or lead various meetings with consortium partners, including:

- Monthly work package meetings
- Monthly progress meetings with the entire consortium
- Ad hoc Working Group Planning Meetings
- Ad hoc Personal Data Protection Meetings
- Meetings and consultations with Advisory Board members and/or External Ethics Committee

A Record of Processing Activities (RoPA), the discussion of issues, advice given, and actions taken will be maintained to track the progress of ethical, security and integrity considerations.

[4] Article 13 of the Grant Agreement

4.4.3. External Ethics Committee

In the collection and processing of data from Data Subjects WW4WL requests research actions that concern highly sensitive and personal issues. An External Ethics Committee (EEC) has been installed to ensure compliance with ethical, security, and integrity requirements.

The EEC comprises of:

- Sona Ftacnikova (Slovak Centre of Scientific and Technical Information, Slovakia)
- Frank Cörvers (University of Maastricht, the Netherlands)
- Rémi Suchon (Catholic University of Lille, France)

The Internal Ethics Advisor (Hans Schmeets) will flag potential issues and deliverables for review by the EEC, which will monitor compliance and offer advice on mitigating issues. This person is also available for additional advice if needed. The EEC meets on an ad-hoc basis.

5. Data types

This chapter is dedicated to outlining WW4WL's data types and data management (Data Registry and Meta data). The basis of this chapter aligns with the Data Management Plan (D1.2) to which it references to a great extent. At the same hand this chapter aligns with important other tools that inform and protect the data of Data Subject. Of main importance is Data Protection Notice (DPN) from MOTUS and the notices from the Data Controllers to operate in line with GDPR and national data act(s).

5.1. Data types in WW4WL

WW4WL recognizes 5 types of data, being project supportive data, (sensitive) personal data, user data, provided and/or secondary data, and research data.

5.1.1. Project supportive data

Project supportive data encompasses any information that is relevant to the project's goals, objectives, and deliverables, and that support the activities done to carry out the project. These documents contain no personal or sensitive data and can be stored on low protected environments or exchanged between consortium members and external parties or persons.

Types of data that are generated as supportive data within the WW4WL project are:

- Website
- Flyers
- Banners
- Deliverables
- (PowerPoint) presentations
- Technical reports
- Meeting reports
- Study protocols
- Articles
- Communication to the public (e.g. via social media)
- Communication to participants

5.1.2. (Sensitive) personal data

The WW4WL project will gather and handle (sensitive) personal data solely when it is necessary for reaching the research goals defined with the WW4WL project proposal. This data is at the core of the WW4WL project and is discussed in more detail in D1.2 Data Management Plan and D3.2 Implementation Plan for Data Collection. This latter deliverable also shows how data is clustered within which datasets.

All in all, WW4WL recognises the following types of (sensitive) personal data:

- **Personal Identifiers**: Information that directly identifies an individual, such as their name, address and email address.
- **Demographic Information**: Data related to an individual's demographic characteristics, including age, gender, and nationality.
- **Financial Information**: Data pertaining to an individual's financial status or transactions as related to the income of an employee or costs for renting an office/building as an employer.
- **Location Data**: Information about an individual's geographic location or movements, including GPS coordinates, or tracking data from mobile devices.
- **Biographical Information**: Details about an individual's personal or professional life, including educational background, employment history, affiliations, or interests.
- **Sensitive Categories**: Certain categories of personal data are considered particularly sensitive and relate to data concerning physical and mental health.

It is crucial to understand that the definition of personal or sensitive data differs according to legal and regulatory frameworks in various jurisdictions. Organizations and researchers must comply with the pertinent laws and regulations concerning the collection, usage, and protection of personal and sensitive data to ensure the privacy rights of individuals are respected and maintained.

If the data upon Data Subjects is received from e.g. companies, schools, associations ..., and/or if data sharing occurs with other national or European partners, a Data Sharing Agreement (DSA) needs to be drafted and signed between the organisations. Having a DSA is the responsibility of each individual party.

5.1.3. User data

User data relates to data that is collected, processed, and used on websites or in apps.

The collection of User data, typically referred to as Cookie data is discussed in the Data Protection Policy of the websites and apps being used within the WW4WL project.

5.1.4. Provided and/or secondary data

The term provided and/or secondary data encompasses two distinct scenarios: data obtained by a partner outside the project and data received from a third-party or a third-party connection (e.g. API). In the first scenario a partner organization involved in the WW4WL project brings in data obtained from outside of the project. This data is then shared or provided to the project for integration, analysis, or further processing, and is included in the project's findings.

In the second scenario data is received from a third party, whether on file or via an API connection. Here the project directly receives data from an external entity or organization that is not formally part of the project consortium or partnership. The data is shared with the project team for specific purposes, such as research, analysis, or implementation, and is included in the project's findings.

In both cases Data Controller, Data Processor, and/or Data Sharing Agreements need to be defined, if applicable. All agreements are listed and stored.

Upon receiving of provided and/or secondary data, the Principal Investigator (PI) will forward the original data to the Data Manager for storage on the server. Research data will then be generated in accordance with the fundamental principles of the General Data Protection Regulation (GDPR) and will be accessible to the PI and researchers as specified in underlying agreements or to those who have signed the Confidentiality Agreement (CA)/Data Sharing Agreement. One database can only contain one type of data and can hold pseudonymised keys for data merging.

All relevant documentation, including the metadata, will be stored on the server.

For the investigation of digital nomads, no third-party data is collected, nor is any data provided by other entities. To collect data for the questionnaire conducted on KoboToolbox, respondents are recruited by posting the questionnaire link on social networks, such as Facebook groups, MeetUp and by posting flyers in coworking and coliving spaces.

5.1.5. Research data

Research data are stored data being received and collected through activities defined within the WW4WL projects' grant proposal and that are processed to be used or analysed to support research findings and validate research results, or are underlying a reasoning, discussion, or calculation in the research.

These research data are anonymised or pseudonymised in a direct manner ensuring that the data cannot be linked back to specific individuals to protect the privacy and confidentiality of research participants while allowing researchers to analyse and share data for scientific purposes.

The research data are discussed within D3.2 Implementation Plan for Data Collection as well as within D1.3 Data Management Plan. D1.3 also continues how the research data is also/becomes subject to the FAIR principles.

Besides data also research output like code and syntaxes to analyse data should be inventoried and stored according to the FAIR principles. The GitHub platform is proposed as collaborative platform.

5.2. WW4WL Data Registry

Each Data Controller or Data Processor has to obligation to keep a Record of Processing Activities (RoPA) providing an oversight of all data (data files) and the processing that is placed upon of these data. Data Managers of the respective partners need to ensure that data is managed efficiently, securely, and in compliance with EU regulations.

To ensure data management, each dataset will possess a unique identifier. Every dataset must be linked to a distinct dataset name to ensure accurate version control.

The identifier for each dataset must be incorporated into the filename, utilizing a common format tailored to the respective data type. Any necessary software requirements will be specified if needed, and will be documented in a Joint DPIA for data processing. Given the project's scope, publicly available software is expected to be utilized for data storage. No interoperability issues hindering access are anticipated.

Following the EU standards, the requirements are:

- To use a Common architecture
- To use a https
- To follow a security architecture aligned with ISO/IEC 270001 standard
- To use a Secured message and certificate formats

Key Features of the Record of Processing Activities strategy are:

- Establishing an online inventory of all data files through a standardized approach, which Data Managers are responsible for maintaining.
- Develop robust security measures to use and share all data types taking into account the GDPR data protection regulations.
- Leverage to the internal Ethics Advisor for requesting information on privacy and security requirements and for exercising control over the provided information.
- Make use of uniform formats and terminologies to ensure data consistency and quality across different partners and datasets.
- Enable integration of data from diverse sources and systems, ensuring that data is interoperable and can be effectively utilized.

Note: WW4WL uses with the MOTUS data collection platform a single platform for all data collections in relation to the employer (survey) and employee study (survey and time diary with geolocations), allowing a uniform approach in collecting data respecting the highest ethical and security requirements. When these data are downloaded from the MOTUS data collected platform in a JSON format these data is registered in the Record of Processing Activities. Once the data are downloaded from the platform the study is deleted, and no information remains on the servers of hbits CV.

Benefits for WW4WL are:

- Streamlined data sharing fosters better collaboration and communication among project partners.
- Standardization processes enhance the reliability and accuracy of collected data.
- Ensures that data handling practices comply with EU regulations, avoiding legal issues and penalties.
- Centralized and well-organized data management processes increase efficiency and reduce redundancy.
- Accessible and high-quality data aids in making informed decisions and advancing project goals.

For the Delphi study a to be defined platform is used, meeting the above criteria.

The obligation to register counts for institutional internal as well as external transfers. This obligation ends when all copies of the data are deleted or fully anonymised (at the maximum 5 years after the end of the project according the DPN) or when the data is (rightfully) published in an open database. When the data is deleted or fully anonymised, this action is documented in the RoPA. When the data are published in an open database, the open database keeps track of the downloads. The Research data form the basis for the actions that will lead to FAIR data. Publicly accessible data hosted on other platforms will adhere to the respective repository's policies, such as those outlined by Zenodo.

Although most of the collected data is expected to be openly accessible and widely disseminated, certain project outcomes may require protection due to intellectual property (IP) rights, as outlined in D1.2 Data Management Plan. This plan will delineate the strategy for managing knowledge and IP emerging from project activities to maximize impact and plan for their exploitation post-project. More information on the applications of the FAIR principles can be found in the Data Management Plan (D1.2).

5.3. Data exchange

WW4WL collects data from employers and employees via surveys and from stakeholders via (Delphi) interviews. In the cooperation between WW4WL partners' data needs to be exchanged in order to be valorised.

WW4WL will conduct a Joint DPIA for the valorisation of data defining how the exchange of data is handled, discussing the roles and responsibilities of each party involved in the data valorisation process as well as the requirements for data storage.

By utilizing a general Data Sharing Agreement, WW4WL creates a structured framework for data exchange while it also helps to maintain transparency and accountability among the parties involved.

5.4. Internal data

Another type of data that is handled within the WW4WL project is the Confidential Data of Consortium members. The following rules apply:

- Consortium Member Confidential Data:

This information is stored on the SharePoint provided by EQY to which all partners have entry.

- Confidential Data Exchange Between Two Consortium Members:

This information is shared on/available from the SharePoint provided by EQY to which all partners have entry.

- Confidential Data Exchange Among All Consortium Members:

This information is shared on/available from the SharePoint provided by EQY to which all partners have entry.

5.5. Meta data

Metadata refers to data that provides information about other data: it is data about data. Metadata can describe various aspects of the data it pertains to, such as its content, structure, format, and context. The details of the meta data have yet to be defined.

6. (Sensitive) personal data

Personal data involve any information capable of directly or indirectly pinpointing an individual's identity or possessing sensitive attributes, necessitating heightened safeguards owing to its potential implications on an individual's privacy, autonomy, or welfare.

Personal data that are considered sensitive[5] are:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person's sex life or sexual orientation.

6.1. (Sensitive) personal data within WW4WL

WW4WL is a project collecting personal and sensitive data. In that case, these data must be collected and processed under Agreement in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/679[6]), or GDPR.

WW4WL partners must ensure that personal data "is:

- processed lawfully, fairly and in a transparent manner in relation to the Data Subjects
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

[5] Article 4 (13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR (Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en#:~:text=personal%20data%20revealing%20racial%20or,sex%20life%20or%20sexual%20orientation.)

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR') (OJ L 119, 4.5.2016, p. 1) (Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1797-1-1)

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data is processed and
- processed in a manner that ensures appropriate security of the data"[7].

These principles are set to be able to pay attention "to:

- the principle of proportionality,
- the right to privacy,
- the right to the protection of personal data,
- the right to the physical and mental integrity of persons,
- the right to non-discrimination,
- the need to ensure protection of the environment and high levels of human health protection"[8].

Data Managers will ensure consistent monitoring of the processing of (sensitive) personal data via the RoPA. WW4WL partners are permitted to allow their personnel access to personal data that is linked to research tasks solely when it is essential for the implementation, management, and monitoring of these research tasks within the WW4WL project. It is the responsibility of the WW4WL partners to ensure that their personnel are bound by confidentiality obligations.

6.2. Informed consent

WW4WL obtains the explicit consent of the Data Subject to which personal and sensitive information is collected. To respect the GDPR principles the WW4WL project draws up tools, guidelines, documents and templates to educate, support and monitor WW4WL partners and persons/researchers through the course of the project to provide the accurate possible information to the Data Subject.

The following elements are of importance for asking consent to participate.

Population

To ensure inclusivity and representation across all activities, researchers will strive for diversity in participants and samples, encompassing various factors such as gender, age, geographic distribution, experience level, regional socio-economic status, and more. Responsible WW4WL partners will ensure the absence of judgement, discrimination, or bias.

[7] Annex 5 of the Grant Agreement
[8] Annex 5 of the Grant Agreement

For activities involving stakeholders, partners will promote research activities on social media platforms and encourage relevant stakeholders to engage.

Procedure

Only individuals who provide prior, voluntary, clear, and informed consent will be involved in WW4WL human-research activities after being identified as potential participants. Specific incentive mechanisms will be provided by the partners. Recruitment and consent procedures will be designed to prevent coercion and ensure voluntary participation, while considering ethical implications such as anonymity, confidentiality, dignity, non-discrimination, non-malevolence, and well-being.

Redress mechanisms will be established to address complaints or concerns raised by individuals or groups negatively affected by WW4WL activities, providing them with avenues to voice grievances and seek remedies.

Before conducting surveys, diary, geotracking or interviews, individuals will be informed in accordance with the informed consent procedures. Consent will also be obtained for all recorded activities and individual responses subsequently utilised in published materials.

WW4WL will process (sensitive) personal data that is collected and subsequently is used within another study of WW4WL. Three different scenarios are apparent in WW4WL.

- Scenario 1: Respondents are re-invited within WW4WL to a study based on a consent given in a previous study within WW4WL.
- Scenario 2: Data Subjects are contacted based on a list with personal data gathered by consortium partners before the WW4WL project.
- Strategy 3: Respondents are contacted based on a contact list from organisations outside WW4WL, to which partners within WW4WL have a contract with, that also includes a Data Sharing Agreement.

Content

Consortium members will provide participants with information sheets and consent forms presented in a language and manner that is fully comprehensible to them. These documents will delineate the objectives, methodologies, and ramifications of the research, as well as the nature of participation and any potential benefits or risks, such as privacy concerns. They will explicitly affirm that participation is voluntary and that participants retain the right to decline participation or withdraw their involvement, including their data, at any juncture without facing any repercussions. Additionally, the forms will elucidate how partners will gather and safeguard data throughout the duration of the project, securely store it, and subsequently delete it.

The project will ensure consistency in the content and communication approach across participant information sheets and consent forms utilized in the WW4WL project, encompassing various activities and study cases.

Language

Partners will strive to communicate with participants in their native languages whenever feasible. In cases where this is not possible, both the information sheet and informed consent form will be translated as needed.

Format

Consent can be provided either online or on paper and will be centrally stored for convenient monitoring by the Internal Ethics Advisor and for ensuring data protection controls.

Obtaining consent

Consent is acquired prior to initiating any activity (such as a survey, session, workshop, panel discussion, etc.) that may raise ethical considerations. After reviewing the information sheet and having the chance to pose questions, participants will grant consent. Written consent will be sought as the default option.

Special considerations

Upon logging into the MOTUS application, users will be presented with a consent check-box stating to have read the MOTUS general Privacy Protection Notice upon answering survey questions, keeping time diaries, and the tracking of positions. In relation to the time-use survey WW4WL will seek permission to track their geographical location for various purposes within the application. Users will have the opportunity to provide or decline consent based on their preferences and comfort levels with geotracking technology. This ensures transparency and empowers users to make informed decisions about their privacy and data usage within the application.

Participants who come across recorded information (whether audio and/or visual) will be furnished with a consent form to review and sign if they are to be photographed, and/or visually and/or audio recorded during project activities.

Storage

Paper consents will be securely stored in file storage facilities at the premises of the consortium members organizing the event to mitigate the risk of loss. Subsequently, these consents will be promptly scanned and transferred to access-restricted folders on WW4WL SharePoint. The physical copies will be securely destroyed upon the conclusion of the project.

As for online consents, they will be retained on the research platforms' servers until the conclusion of the respective event. Afterward, they will be transferred to the project's SharePoint, where access will be restricted to specific consortium members with designated permissions and protected by passwords. Subsequently, these consents will be permanently deleted from the research platform's environment.

Deletion

After the project concludes, electronic copies of the consents will be retained by the Principal Investigator for a duration of up to 5 years. This retention period is following EC (European Commission) requirements and aims to assist Data Subjects who may wish to exercise their rights during this timeframe.

6.3. Ensuring Data subjects' rights

Data subjects are asked participation based on a Privacy Declaration Notice and an information sheet. Afterwards, these participants can claim rights in accordance with the General Data Protection Regulation (GDPR). These rights are:

- Right of Access: Participants may request access to their personal data held by the project.
- Right of Rectification: Participants may request the correction of any inaccuracies in their personal data.
- Right of Erasure: Participants may request the deletion of their personal data.
- Right to Restriction of Processing and Objection: Participants may request limitations on future processing of their personal data or object to its processing.
- Right to Data Portability: Upon request, participants will receive a copy of their data in a structured, commonly used, and machine-readable format.
- Right to Withdraw Consent: Participants may withdraw their consent at any time, thereby halting further processing activities.
- Right to Object against automated decision-making and profiling.
- Right to Lodge a Complaint: Participants have the right to lodge a complaint with a supervisory authority.

In case of a data collection, the MOTUS research platform provides a General Privacy Notice while the various case studies provide a more specific Privacy Declaration Notice.

The KoboToolbox platform, used by IST-ID to collect data for various studies and projects, has its own General Privacy Notice (KoboToolbox, 2025e), available to any interested party, and provides respondents with integrated mechanisms that allow:

- Right of Access
- Right of Rectification
- Right of Erasure
- Right to Data Portability
- Right to Withdraw Consent
- Right to Object
- Right to Lodge a Complaint
- Among other rights provided for in the General Data Protection Regulation (GDPR)

These rights are directly accessible to participants who have their own account on the KoboToolbox platform, who have submitted their answers through that account.

Respondents without an account but who have given their email address can exercise their rights by contacting the Data Manager, via:

- The KoboToolbox platform itself (if applicable)
- The e-mail addresses provided in the study's Informed Consent or Privacy Statement

In these situations, the Data Manager team – currently the Master's student Beatriz Cardoso, in collaboration with Professor João de Abreu e Silva (the person formally responsible for research at the IST-ID centre) – will be able to carry out the necessary actions manually, such as:

- Deleting data from the study database
- Providing a copy of the data submitted
- Limiting further processing of the data

Anonymous respondents are the most common types of respondents for IST-ID and participate to studies via an anonymous link and provide no personal data (e.g. email address). This data is stored anonymously and cannot be retrieved.

All requests received will be handled with due diligence and within the legal deadlines, ensuring compliance with the GDPR (KoboToolbox, 2025e).

6.4. Process of pseudonymisation and anonymisation

(Sensitive) personal information can be used as research data when it has been anonymised following the ethical principles and legal requirements by carefully remove or obscure identifying information and safeguarding the privacy of research participants while allowing for meaningful analysis and dissemination of research findings.

6.4.1. Anonymisation

Anonymisation is the process of removing or altering identifying personal data from data sets to protect the privacy and confidentiality of data subjects. The following strategies to achieve anonymisation can be applied:

- **De-identification of Personal Information**: Anonymised research data involves removing or altering any identifying information that could potentially link the data to individuals. This includes names, addresses, phone numbers, email addresses, social security numbers, and any other identifiers. Additionally, sensitive information such as dates of birth or specific geographic locations may be generalized or aggregated to further protect anonymity.
- **Pseudonyms**: Anonymisation may involve randomizing or coding data to obscure any direct linkages to individuals. For example, assigning unique

identifiers or pseudonyms to participants can help researchers track data without revealing personal identities.

- **Aggregation and Generalization**: Another approach to anonymisation involves aggregating data or generalizing it to broader categories. Instead of reporting individual responses, researchers may present summarized statistics or trends across groups to prevent the identification of specific individuals.
- **Contextual Considerations**: Anonymisation also takes into account the context of the data and potential re-identification risks. Researchers must consider not only the direct identifiers but also any indirect identifiers or combinations of variables that could lead to the identification of individuals.

6.4.2. Pseudonymisation

Pseudonymisation is a data protection technique that replaces or removes direct identifiers from personal data, substituting them with artificial identifiers or pseudonyms. The purpose of pseudonymisation is to enhance data privacy and security while still allowing for data processing for legitimate purposes. The following strategies can be applied:

- **Protects Identity**: Pseudonymisation obscures the direct link between personal data and the individual it pertains to. By replacing identifiable information such as names or social security numbers with pseudonyms, it makes it more difficult to identify individuals from the data alone.
- **Reduces Re-identification Risk**: Even if pseudonymised data were to be compromised or accessed by unauthorized parties, the risk of re-identifying individuals is significantly reduced compared to if the data were left in its original identifiable form. This helps mitigate privacy risks associated with data breaches or unauthorized access.
- **Facilitates Data Processing**: Pseudonymisation allows organizations to process personal data for various purposes, such as research, analysis, or sharing, while still adhering to data protection regulations. It enables data to be used for legitimate purposes without compromising individuals' privacy rights.
- **Enables Data Linkage**: Despite removing direct identifiers, pseudonymisation allows for the linkage of data records belonging to the same individual across different datasets or systems. This can be valuable for data analysis, research, or integration purposes while still maintaining privacy.
- **Supports Data Governance**: Pseudonymisation is often used as part of broader data governance and privacy protection strategies. By pseudonymising personal data, organizations demonstrate their commitment to protecting individuals' privacy and complying with data protection regulations.
- **Balances Privacy and Utility**: Pseudonymisation strikes a balance between protecting privacy and maintaining the utility of the data for legitimate purposes. It allows organizations to derive insights and value from data while minimizing privacy risks and ensuring compliance with legal requirements.

It's important to note that while pseudonymisation enhances privacy and security, it is not foolproof. In some cases, combined with other information, pseudonymised data may still be re-identified. Therefore, WW4WL is committed to have implemented additional safeguards and controls to complement pseudonymisation, such as access controls, encryption, and strict data handling policies, to ensure robust data protection.

Related to the above, the MOTUS data collection platform makes use of UUIDs or a Unique number as keys to exchange information within the platform and its components, and between external environments that are linked to the platform via an API.

The data provided to KoboToolbox and to the Data Manager is anonymised, and does not include direct identifying elements (such as name, email or other contact details). KoboToolbox offers the possibility of responding to surveys without having an account or providing identifying information (such as email address or name) and IP addresses (KoboToolbox, 2025f).

7. Data security

Scientific research frequently utilizes personal data. Adopting the Research Principles also means ensuring the security of data. Whether it concerns personal or sensitive information, research data, financial records, meeting and attendance reports, or intellectual property, safeguarding data against unauthorized access, theft, or corruption is paramount.

To secure this data WW4WL puts efforts to two domains. WW4WL establishes minimum standards for the collection, processing, storage, and deletion of (sensitive) personal and other data. Subsequently, it elucidates the organisational and technical measures project members will need to follow to safeguard these data and to uphold the rights of Data Subjects. Specific requirements will be listed in the agreement of a Joint DPIA for the valorisation of data.

7.1. Principles for processing (sensitive) personal data

All personal data must be handled appropriately, regardless of the method of collection, recording, or processing—whether it's on paper, online, stored in a computer file or database, or recorded on any other material. There are widely recognized principles where upon the GDPR regulation is based and which are updated in the latest Ethics Self-Assessment guide taking into account new online and AI/ML realities.

These principles are separately and all together addressed in various documents (DMP, DPIA, Privacy Declaration Notice, ethical approvals, ...) that are produced during the WW4WL project making all partners within the project aware of these principles and the need to be able to demonstrate that they actively took or take responsibility for the secure processing of (sensitive) personal, as well as other data. By implementing these strategies effectively, WW4WL partners and their personnel can mitigate risks and protect personal and sensitive information from potential threats.

Below these principles are addressed.

Principle 1: Lawful basis, fairness and transparency

All Data Collectors, Data Processors, and Data Users within WW4WL will have to inform themselves about the GDPR, international and national regulation to remain lawful. Even though it might be lawful, fairness is achieved by considering how the processing of (sensitive) personal data can affect the Data Subjects concerned. Transparency is achieved by clearly stating in the consent, information sheet and privacy statement which data is gathered and for what reason and how the collected data is processed. Also, the involved parties are communicated to the Data Subject.

The DPOs of the project members need to decide whether a Data Protection Impact Assessment needs to be conducted.

Principle 2: Purpose limitation

Data purpose limitation is a principle in data protection and privacy that states that (sensitive) personal data should only be used for the specific purpose for which it was collected and no other purposes. WW4WL will therefore not process (sensitive) personal data for new or incompatible purposes for which the Data Subject has not given consent, or which are not permitted by law. With data purpose limitation it is ensured that Data Subjects have control over how their personal information is used, and to prevent researchers from using personal data for unintended or unauthorized purposes.

Principle 3: Data minimization

Data minimization is a principle in data protection and privacy that states that data should be collected, processed, and stored only to the extent that it is necessary to achieve the specific purpose for which it was collected. WW4WL will as such only collect the minimum amount of data necessary to achieve research goals. With data minimization the risk of harm to individuals is reduced by limiting the amount of sensitive or personal information that is processed, stored, and transmitted.

Principle 4: Data accuracy

Data accuracy refers to the degree to which data correctly reflects the real-world information it is intended to represent. In other words, data accuracy refers to the correctness and completeness of data. WW4WL will put data validation and quality control processes in place, and if needed data will be regularly reviewed and updated. Maintaining accurate data is a critical aspect of responsible data management, as it helps to ensure that decisions based on the data are sound and that the data can be trusted for its intended use.

Principle 5: Data storage limitation

Data storage limitation states that personal data should not be stored for longer than is necessary to achieve the specific purpose for which it was collected. WW4WL will delete or dispose personal data that is no longer needed for the original purpose, and at least 5 years after the end of the project unless there is a legal requirement to retain it for a longer period. With storage limitation the risk of harm to individuals is reduced by minimizing the amount of time their personal information is processed, stored, and transmitted.

Principle 6: Confidentiality and agreement

Data confidentiality and agreement refer to the obligations and responsibilities to protect the confidentiality of sensitive or personal information. WW4WL ensures that no person is allowed to access personal data without authorization. It ensures the protection against unauthorized and unlawful processing. This includes the encryption and pseudonymization of personal data wherever possible.

7.2. Accountability

Accountability relates to taking appropriate technical and organizational measures. WW4WL will therefore take accountability in adopting to data protection policies, maintain documentation of one's processing activities, and adhering to relevant codes of conduct. This also includes recording and, where necessary, reporting personal data breaches.

An important tool is the RoPA which needs to reflect to storage of each dataset containing personal data or other data, and is hold by each project member.

Another important pre-processing tool is the study protocol which documents all the steps that are taken in relation to the collection of data from the Data Subjects. Modifications to the study protocols are documented in on the SharePoint.

7.3. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process designed to help project partners to systematically analyse, identify, and minimize the data protection risks of a project or plan. Article 35 of the GDPR requires conducting a Data Protection Impact Assessment (DPIA) in situations where there is a significant risk to the rights and freedoms of individuals. In WW4WL this relates to the participation of individuals to data collection.

The link as addressed below shows the publication of the European Data Protection Supervisor (EDPS), in collaboration with the national protection authorities within the EU. This document makes use of flowcharts and checklist to define whether or not a DPIA is necessary and who has to perform a DPIA (https://www.edps.europa.eu/sites/default/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf.)

7.3.1. Rationale of a DPIA

By conducting a DPIA the aim is to demonstrate compliance to the GDPR and so to ensure that privacy and data protection risks are effectively managed. It offers a structured approach to identifying risks and implementing protective measures by analysing the planned processes. Moreover, it identifies security risks separate from privacy concerns. Sketching out all processes, and contexts to these processes helps to pose the right questions. The study protocols therefore are a vital element in the entire monitor.

WW4WL recognises research actions and study scenarios that demand from Data controllers in collaboration with Data processors to define a DPIA. This is particularly relevant given the WW4WL proposed data collection and processing activities involving:

- Systematically monitoring, tracking, and observing individuals' location and behaviour.

- Combining, linking, or cross-referencing disparate datasets, where such linking significantly contributes to or is utilized for profiling or behavioural analysis of individuals.

WW4WL integrate the measures outlined in these DPIAs into existing legal and ethical frameworks to define responsibilities within WW4WL and for the partners within their own institutions.

7.3.2. Roles in the DPIA

Article 35 of the GDPR mandates that the responsibility for conducting a DPIA lies with the Data controller. In the WW4WL consortium a Data controller is an institutional partner who needs to comply with the legal requirements of data protection. When two or more controllers determine the purposes and means of processing these controllers are labelled Joint Data controllers.

- **Data processors** within WW4WL are institutional partners who processes (sensitive) personal data in place of the Data controller without having control over the purposes and means of the processing operation. Data processers are required to assist the controller in complying to the DPIA.
- **IT service providers** that provide software and/or hardware components are technically responsible for parts of the data processing operations. Service providers are assumed to take an active role in the definition of, and compliance to, a DPIA. The level of assisting is related to the amount of operational freedom the Data controller has within the provided IT service. Depending on this analysis a Data processor agreement is developed.

Working with IT service providers often means transmitting personal data to the platforms to furnish samples, or to enrich existing ones. To ensure IT systems can adhere to these client-specific restrictions or requirements, it's crucial that such instructions are formally documented and agreed beforehand.

7.4. Privacy and Security on the technical level

By taking all necessary steps and by attaching responsibilities to roles within the WW4WL consortium the principle of ‘data protection by design’ should effectively mitigate possible risks.

Protection measures like pseudonymisation or encryption are generally seen as important measures in the GDPR, but new realities and new data collection methods challenge the task to be compliant. Therefore, also IT service or systems are discussed in view of privacy and security by design and by default, in their support of a privacy-conscious culture within organisations. The more an IT service can protect the privacy and security of data on a technical level, the better the GDPR principles can be guarded. Building safeguards into IT systems that protect the rights of participants are therefore essential.

7.5. Privacy by design

Privacy by design on an IT level envisions the promotion of IT systems that prioritize the protection of individuals' privacy rights from the outset, from the initial design to deployment and beyond. Privacy here is an integral part of the architecture itself. This is done by:

- Designing and implementing a software application architecture that organises applications in logical and physical tiers each running on its own infrastructure (presentation tier, application tier, data tier).
- Using encryption and pseudonymisation to protect from reading by other the confidentiality of personal data during storage, transmission, and processing.
- Implementing access controls to restrict access to personal data to authorized personnel only, based on the principle of least privilege.
- Implementing measures to ensure the integrity and security of personal data, such as data backup, regular security assessments, and incident response plans.
- Conducting security and performance tests to prove the hardness of the IT system.
- Develop a supportive user interface for researchers that is clear and easily to understand to support their tasks in protection data security and data quality.

For many years, the dominant architecture for client-server applications was the three-tier architecture. Nowadays, most of these three-tier applications are being considered for updates, leveraging cloud-native technologies like containers and microservices, and for transitioning to cloud-based environments.

At WW4WL the preference is made to collect data via one IT-platform, being the MOTUS data collection platform.

KoboToolbox, when used on its European server infrastructure, aligns with GDPR by design and by default regarding data location, secure transmission, and server management practices. Nevertheless, additional measures – such as careful survey design to avoid unnecessary collection of personal identifiers – are essential to fully implement privacy by design principles in data collection projects (KoboToolbox, 2025g). Privacy here is also an integral part of the architecture, done by:

- Designing and implementing a software architecture that separates the system into logical tiers (frontend and backend) running on a secure infrastructure within the European Economic Area (EEA). When using the European server, data remains stored and processed entirely within the EEA in compliance with the General Data Protection Regulation (GDPR).
- KoboToolbox ensures the encryption of data during transmission through HTTPS/TLS protocols.
- KoboToolbox offers permission management that allows project owners to limit access to datasets and administrative features.
- Implementing measures to ensure the integrity and security of personal data, such as data backup, regular maintenance, security updates, and incident response processes. The European KoboToolbox servers provide regular data

backups and follow security management practices aligned with GDPR requirements, including breach notification procedures.
- Conducting security and performance tests to prove the hardness of the IT system.

7.6. Privacy by default

This principle aims to ensure that individuals' privacy is safeguarded by default. On an organisation level this means adopting the highest privacy protection in adhering the research principles, like e.g. agreeing to a short storage period.

It also would mean e.g. not to track the behaviour when public webpages are visited, and to use only necessary and functional cookies. It also means that users should not actively opt out of invasive data collection settings but rather opt-in on a consent and trust-based level to collect data via internal sensors. It would also mean that users can consult the collected data via the applications that are being used during the study.

For WW4WL it means that participation to a study is not only based on free will but also with supporting participants' confidence the participation starts with a set of minimal requests, and that in the continuation of building up confidence proceed to collecting more highly detailed data even through sensors or the merging with other databases. Participation to the studies without accepting active sensors remains possible to avoid discrimination.

Via the MOTUS data collection platform WW4WL, and the front-office applications the privacy by default setting can be achieved.

KoboToolbox, when in the European server (as in the case of the digital nomads survey), does not track visitor behaviour on public pages of the platform. The cookies used are essentially functional, necessary to maintain authenticated user sessions or for the basic operation of the platform. No tracking or marketing cookies are used. KoboToolbox also does not collect data by internal sensors or devices (e.g. GPS, accelerometer, etc.) by default. Any collection of this type of data depends on the design of the form made by the researcher: if the form does not request location or other sensitive information, it will not be collected; here, consent and choice are implemented in the logic of the form and in the informed consent process prepared by the researcher (KoboToolbox, 2025e).

7.7. Data storage

Storage facilities are an important technical aspect to keep (sensitive) personal data private and secure. Whether an institution is a Data Controller, Data Processor or Data User the architecture upon which the data is stored is of importance.

Data collected and processed by project partners is to be stored on reliable environments. WW4WL makes a distinction between data storage during data

collection, data storage that is archived in order to be valorised by the different partners, and data that is made available open source following the FAIR principles.

More detail is provided below.

7.7.1. Data storage during data collection

WW4WL data collection is labelled as a high risk for reasons of dealing with (sensitive) personal data, for the types of data, for the (continuous) interaction with Data Subject, for the amounts of data but also in the transfer (internal/external) of data. At various places data could be breached to the outside world.

To minimize risk on breaching data, the WW4WL project chooses to make use of only two data collection platforms, being the MOTUS data collection platform and the platform to conduct Delphi studies.

MOTUS data collection platform

MOTUS has been developed privacy and security by design. Data storage is defined to be privately hosted, ISO27001 certified, and entry is restricted through role management and 2-factor authentication. Data storage need to be on a different server than the other processes.

The complex data collection design has to map the internal exchange of data based on UUID-keys. For the transmission an encoding standard is needed to transmit (pieces of) data between the internal components. External exchange of data needs to be encrypted and transferred over a https protocol with an SSL/TLS encryption layer. In the private/secure exchange of data a relational database is needed for a fluent exchange. The server hosting the database needs to be performant, up-to-date and the security level needs to be monitored. Actions need to be in place to protect against DDoS attacks.

Different databases are available for personal data, research data and data that is collected via automated processes (e.g. sensory data). A back-up is taken from the databases, running on the internal network only.

Data can be exported on role definition, and when following user agreements.

KoboToolbox data collection platform

The IST-ID data collection using KoboToolbox is treated with due diligence since respondents may have provided their email addresses, due to the types and volume of data collected (since it is expected to receive 1000 responses to this questionnaire), and due to the transfer (internal/external) of data. At various points in the process, there is a risk of data breaches to the outside world. To minimize the risk of data breaches, the IST-ID project make use the KoboToolbox platform hosted on its European server, which is explicitly designed to comply with the General Data Protection Regulation (GDPR).

KoboToolbox (EU server) provides secure data storage within the EEA. Data is transmitted via HTTPS/TLS encryption and stored on protected servers managed under GDPR standards (KoboToolbox, 2025e).

Access is controlled via project-based role definitions (namely the IST-ID PI and the researcher involved in the digital nomads case study) Internal data exchange occurs securely within the platform infrastructure. Separation between personal data and research data must be ensured by project design. External data exports require authorised roles and must follow internal data handling and encryption protocols.

The platform manages server maintenance, security updates, backups within the EEA, and protection against common threats at the hosting level. Data exports are only possible according to role definitions and in line with user agreements (KoboToolbox, 2025e.

Delphi study platform

This platform is going to be selected in the next phase of the WW4WL project.

7.7.2. Data storage for archiving and valorisation

Data that have been collected are archived upon completion of the collection period and subsequent processing (i.e. data cleaning, data valorisation within the WW4WL project) by various partners.

To support this process a Joint DPIA for valorisation data is defined under the leadership of LISER. This DPIA will also provide the requirements of the institutional hardware to be used by the different WW4WL partners to storage databases.

A table (in the next version) will be drawn showing the storage hardware of every project member.

Research data is only available to researchers from their own institutional hardware and is role protected. Research data in active use can be stored on the local drives of researchers' computers or external drives but cannot not be synchronized with any external third-party cloud services different from those which are used as archiving hardware. All data processing activities are meticulously documented in syntaxes.

The European Union's KoboToolbox server stores the data on Amazon Web Services (AWS) servers. There are two types of data stored on these servers: the form itself and the attachments related to each submission (KoboToolbox, 2025h. The form data is saved in the database and the attachments are saved in the Simple Storage Service. The data stored in the database will be deleted according to the stipulations in the Data Management Plan. The same counts for the data collected on the storage service. As agreed within the WW4WL policy, all data, including the data stored on IST-ID's local servers will be deleted by 2027 for raw data and pseudonymized cleaned data in 2032.

7.7.3. Data storage on open access repositories

WW4WL has selected ZENODO as its open-access repository. ZENODO serves as the open-access repository for the Open Access Infrastructure for Research in Europe (OpenAIRE).

The submitted data files will have unrestricted access, as there are no confidentiality or Intellectual Property Rights (IPR) issues associated with them. All collected datasets will be made available having an embargo period. Further information is to be found in the D1.2 Data Management Plan under section 3.2.

7.8. Security management

Security management involves implementing practices, processes, and strategies to safeguard an organization's assets, resources, and information from potential threats, risks, and vulnerabilities. It includes systematically identifying, assessing, mitigating, and monitoring security risks to maintain the confidentiality, integrity, and availability of essential resources.

7.8.1. Entrance and role management

WW4WL employs an entrance and role management to establish a robust security framework to safeguard against unauthorized access to its digital environments. By incorporating two-factor authentication (2FA), an extra layer of security is added to the authentication process, requiring two forms of verification. WW4WL recommends using an authentication app for this purpose.

Access to certain parts of the environment is restricted based on user roles. Effective role management ensures that users have the appropriate level of access according to their responsibilities, thereby maintaining security and compliance.

In ANNEX 2 the various access levels are described.

7.8.2. Security awareness and training

WW4WL will train researchers in security awareness, to support them in security best practices, threats and into their specific role in maintaining security.

7.8.3. Incidence response and management

WW4WL will discuss protocols and procedures for detecting and responding to security incidents (see ANNEX 4). Data breaches have to be reported within 72 hours to the DPO of the respective institution and to the WW4WL internal ethics committee.

Incidence response and management also deals with the after care and analysis of data breaches.

7.8.4. Security management and surveillance

WW4WL trusts upon the implementation of tools and technologies for continuous monitoring of systems, networks, and applications to detect and respond to security threats in real-time.

7.8.5. Additional mitigation strategies

Additionally, WW4WL mitigates the risk of data leaks by:

- For local storage, maintaining data redundancy by storing in at least two separate locations of which the LISER data storage is one of the two locations.
- For version control, keeping the LISER data storage version as the calibration version.
- For cloud storage, select a solution with safeguards against accidental removal, such as a recycle bin feature.

8. Research integrity

In the WW4WL, the goal is to achieve the highest quality of research on Remote Working Arrangements. This is accomplished by integrating data collected from employers, employees, and stakeholders with a combination of classic and innovative research methodologies to address key arising research questions. To support this general goal of the WW4WL project the ALLEA Code of Conduct is combined with the GSBPM process architecture developed by UNECE, Eurostat and OECD as a statistical step-by-step process of collecting data.

8.1. ALLEA and GSBPM

Research integrity is crucial for maintaining the credibility and reliability of research. The ALLEA (All European Academies) Code of Conduct for Research Integrity provides comprehensive guidelines to reach these principles.

The ALLEA Code of Conduct is structured around four fundamental principles and several good research practices:

- **Reliability** in ensuring the quality of research
- **Honesty** in developing, undertaking, reviewing, reporting, and communicating research in a transparent, fair, full, and unbiased way
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage, and the environment
- **Accountability** for the research from idea to publication, for its management and organisation, for training, supervision, and mentoring, and for its wider impacts

The GSBPM offers a structured framework for the processes involved in generating official statistics, organized into phases and sub-processes that steer the development, production, and dissemination of statistical data.

The image below illustrates a reference model that can be used to map actual business processes. This mapping helps describe activities and align them with their typical inputs and outputs, which is essential for collaborative projects like WW4WL that focus on innovative approaches to data collection, valorisation, and reporting in policy documents. All in connection to respondents, and stakeholders, but also to researchers that are employed within different phases of the GSBPM.

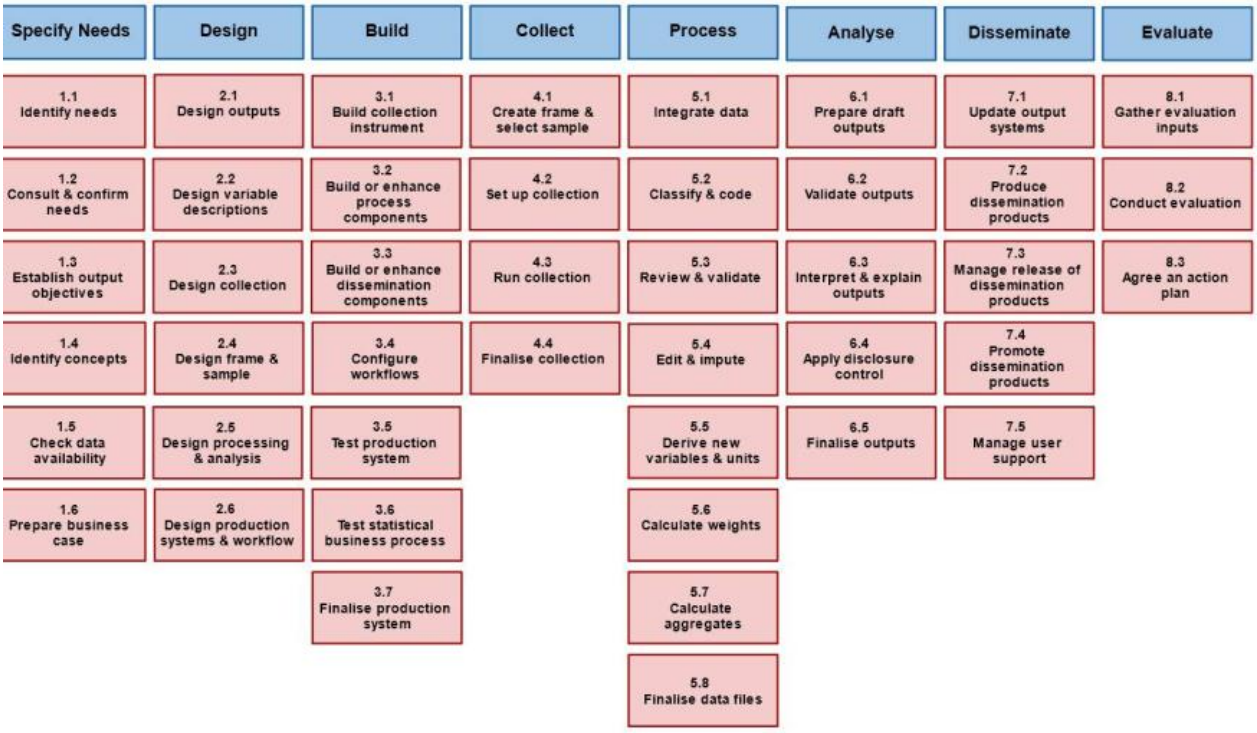

Figure 2: Generic Statistical Business Process Model

8.2. GSBPM mapped on research integrity principles

The GSBPM outlines eight phases that can be aligned with the research integrity principles set by ALLEA. For the WW4WL project, this alignment ensures that every stage of the research adheres to ethical standards and promotes transparency. Here's how each phase connects to these principles:

Phase 1: Specify Needs

Defining clear and necessary research objectives is crucial. Transparent communication about the research's scope and purpose ensures that all stakeholders understand its relevance and necessity. Ethical considerations must be integrated into the needs assessment, ensuring the rights and well-being of participants are respected throughout the project.

Phase 2: Design

The design phase focuses on creating robust, reproducible research methods that align with the research questions. This involves developing protocols that minimize biases and ensure the validity of the research. Comprehensive documentation of the design process is essential to facilitate peer review and enable replication, reinforcing the credibility of the research.

Phase 3: Build

In this phase, the necessary tools and infrastructure for data collection and analysis are constructed with a strong emphasis on adhering to ethical standards, particularly regarding data security and privacy. It is crucial that all team members understand their roles and responsibilities, with mechanisms in place to ensure accountability and integrity throughout the project.

Phase 4: Collect

Data collection must be conducted ethically, with strict adherence to informed consent, confidentiality, and the protection of sensitive information. Quality control measures are implemented to ensure the accuracy and reliability of the data collected, safeguarding the integrity of the research.

Phase 5: Process

During data processing, it is vital to avoid introducing errors, biases, or manipulation. Responsible handling of data includes careful cleaning, coding, and transforming, with detailed records maintained for every step to ensure reproducibility and verification. This phase emphasizes the importance of accuracy and transparency in data handling.

Phase 6: Analyse

Analyses are conducted objectively and based on sound statistical methods, with a commitment to avoiding data dredging or p-hacking. Results are reported honestly, including any negative findings, ensuring that the research does not selectively present data to support a predetermined outcome. This phase is critical for maintaining the objectivity and credibility of the research.

Phase 7: Disseminate

Results are shared openly and transparently, including detailed methodologies, data sources, and any limitations of the research. This phase ensures that the dissemination of findings is accurate and does not mislead or misrepresent the research to the public or the scientific community, upholding the integrity of the project's conclusions.

Phase 8: Evaluate

Continuous evaluation of the research process and outcomes is essential to identify areas for improvement. This includes engaging in peer review, conducting replication studies, and addressing any issues that arise. Researchers take full responsibility for the research process and outcomes, including the rectification of any errors or ethical breaches identified during the evaluation phase.

By aligning each of these phases with the principles of research integrity, the WW4WL project ensures that its processes are not only methodologically sound but also ethically robust, fostering trust and credibility in its findings.

8.3. Respect for colleagues

Respect for colleagues is a cornerstone of successful collaboration, particularly within the context of EU-funded projects, where diverse teams come together from various countries, cultures, and disciplines. These projects, often large in scale and complexity, require a high level of cooperation and mutual understanding to achieve their objectives. Fostering an environment of respect among colleagues is not only essential for maintaining morale and motivation but also for ensuring that the project meets its goals effectively and efficiently.

Understanding diversity and inclusion

EU-funded projects bring together individuals from across Europe and sometimes beyond, each contributing their unique perspectives, skills, and experiences. This diversity is one of the greatest strengths of such projects, but it also requires a conscious effort to foster an inclusive environment. Respect for colleagues begins with acknowledging and valuing these differences, recognizing that diverse viewpoints can lead to more innovative solutions and richer project outcomes. Inclusion means ensuring that all voices are heard and respected, regardless of nationality, gender, language, or professional background.

Effective communication

Clear, open, and respectful communication is vital in any collaborative effort, and it is especially critical in the multilingual and multicultural environments of EU-funded projects. Misunderstandings can arise from language barriers or cultural differences, so it is important to be patient, clarify meanings, and ensure that all parties feel comfortable expressing their thoughts and concerns. Active listening, where team members truly engage with what their colleagues are saying, is an essential aspect of respectful communication.

Collaboration and teamwork

Respecting colleagues also means valuing their contributions to the project. In a team setting, this involves recognizing and appreciating the efforts of others, sharing responsibilities equitably, and being willing to offer support when needed. Collaboration in EU-funded projects often requires a high degree of interdependence among partners, making it crucial to trust each other's expertise and to work towards common goals. Respectful collaboration fosters a sense of shared ownership over the project's success and creates a positive working environment where all team members can thrive.

Conflict resolution

In any collaborative project, conflicts may arise. How these conflicts are managed can significantly impact the overall success of the project. Respectful conflict resolution involves addressing disagreements openly and constructively, seeking to understand the other person's perspective, and finding mutually acceptable solutions. It's

important to address issues promptly and professionally, without letting them escalate or become personal. In EU-funded projects, where teams may be spread across different countries, maintaining respect in virtual communication is also crucial to preventing misunderstandings and resolving conflicts effectively.

Ethical considerations

Respecting colleagues extends to upholding ethical standards in all aspects of the project. This includes ensuring transparency in decision-making, protecting confidential information, and giving credit where it is due. Ethical behaviour also involves respecting the intellectual property and contributions of all partners, as well as ensuring that all project activities comply with the legal and ethical guidelines established by the EU.

Promoting a positive work environment

A positive work environment is one where respect is not only practiced but encouraged and reinforced at all levels. Leadership within the project plays a critical role in setting the tone for respect and inclusion. Leaders should model respectful behaviour, encourage collaboration, and address any issues of disrespect or exclusion promptly. At the same time, all team members have a responsibility to contribute to a respectful and supportive work environment, where everyone feels valued and motivated to contribute their best work.

9. Conclusion

The Ethical and Security Management Report (ESMR) aims to provide the tools and methodologies necessary for managing the data collected, generated, and processed throughout the WW4WL project. This document will be regularly updated during the project to address new requirements and integrate evolving regulations, ensuring adherence to ethical standards, resource efficiency, and data security.

All work packages (WPs) within the project must follow the guidelines established in the ESMR, integrating them into their activities. Compliance with the ESMR is mandatory for all WW4WL members, including every partner involved in the project.

10. Bibliography

KoboToolbox (2025a). *About the Kobo Organization*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/about-us/the-organization/

KoboToolbox (2025b). *About us*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/about-us/

KoboToolbox (2025c). *Features*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/features/

KoboToolbox (2025d). *Data Security*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/features/data-security/

KoboToolbox (2025e). *Privacy Notice*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/privacy/

KoboToolbox (2025f). *Collecting IP addresses*. KoboToolbox Community. Retrieved on 7 July 2025, from https://community.kobotoolbox.org/t/collect-ip-address-from-web-data-entry/37530

KoboToolbox (2025g). *Support KoboToolbox*. KoboToolbox Support. Retrieved on 7 July 2025, from https://support.kobotoolbox.org/gdpr.html

KoboToolbox (2025h). *Data Storage*. KoboToolbox. Retrieved on 7 July 2025, from https://support.kobotoolbox.org/data_storage.html

KoboToolbox (2025i). *Terms of service*. KoboToolbox. Retrieved on 7 July 2025, from https://www.kobotoolbox.org/terms/#:~:text=Usage%20Data%20Kobo%20may%20use%20data%20related,of%20confidentiality%2C%20as%20permitted%20by%20applicable%20law.

KoboToolbox (2025j). *Permissions*. KoboToolbox. Retrieved on 7 July 2025, from https://support.kobotoolbox.org/managing_permissions.html

ANNEX 1: Ethical and Security Considerations during the WW4WL project

Project partners acknowledge following the Ethical and Security Management Report (ESMR) defined for the WW4WL project. This also means being familiar with the guidelines on completing your ethics self-assessment for applicants and beneficiaries of EU projects of the European Commission to which the main report (Deliverable 1.3) provides an answer to, to the request to define research protocols (ANNEX 3) and to be informed by the Code of Conduct as set out by the European Commission and published by ALLEA[9].

The following is an overview of the considerations each consortium researcher must take into account. Incorporating these ethical and security considerations into project planning and execution helps ensure that the project aligns with societal values and protects against potential risks.

1. Ethical Considerations for WW4WL

When carrying out a project, particularly one involving research or data collection, it is essential to consider a range of ethical issues to ensure that the project is conducted responsibly and respectfully.

1.1. Privacy

- Ensure the confidentiality of personal and sensitive information.
- Collect only necessary data and obtain consent for its use.
- Implement robust data anonymisation and pseudonymisation techniques where applicable.

1.2. Bias and Fairness

- Identify and mitigate biases in data collection and algorithm design.
- Strive for inclusive and fair treatment of all user demographics.
- Regularly audit systems for unfair treatment or discrimination.

[9] ALLEA : All European Academies - https://allea.org/portfolio-item/european-code-of-conduct-2023/

1.3. Transparency

- Clearly communicate the purpose, scope, and impact of the project.
- Make methodologies and decision-making processes understandable to stakeholders.
- Provide transparency reports and documentation for public review.
- Keep an updated data registry showing who and how data is used.

1.4. Accountability

- Assign responsibility for ethical decision-making within the project team through data agreements attached to roles like (Joint) Data controllers, Data processors, and Data users following the Flowchart and checklists on Data Protection of EDPS[10].
- Implement mechanisms for reporting and addressing ethical concerns.
- Hold developers and project managers accountable for ethical breaches.

1.5. Informed Consent

- Ensure that users understand what data is being collected and how it will be used.
- Provide clear, accessible consent forms and privacy policies.
- Respect user autonomy and their right to withdraw consent.

1.6. Impact on Society

- Consider the broader societal implications of the project.
- Avoid actions that could harm public welfare or contribute to negative societal outcomes.
- Engage with community stakeholders to understand and address their concerns.

2. Security Considerations for WW4WL

When conducting a data collection project, it is crucial to consider various security measures to protect the data and ensure the integrity of the research process.

2.1. Data Protection

- Implement strong encryption for data at rest and in transit.

[10] EDPS – European Data Protection Supervisor : https://www.edps.europa.eu/sites/default/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf

- Regularly update and patch systems to protect against vulnerabilities.
- Utilize secure coding practices to prevent common vulnerabilities such as SQL injection and XSS.

2.2. Access Control

- Enforce the principle of least privilege, granting only necessary access to data and systems (ANNEX 2).
- Implement multi-factor authentication (MFA) for accessing sensitive information (ANNEX 2).
- Monitor and audit access logs to detect and respond to unauthorized access.

2.3. Incident Response

- Develop and maintain an incident response plan to address security breaches (ANNEX 4).
- Regularly test and update the Incident Response Plan through simulations and drills.
- Ensure timely communication and remediation steps in the event of a security incident.

2.4. Risk Management

- Conduct regular risk assessments to identify and prioritize potential threats.
- Develop mitigation strategies for identified risks.
- Stay informed about emerging security threats and adapt strategies accordingly.

2.5. Compliance

- Adhere to relevant laws, regulations, and standards, such as GDPR.
- Maintain comprehensive records of compliance efforts and audits.
- Stay updated on changes in legal and regulatory requirements.

2.6. Security Training

- Provide regular security training for all project team members.
- Promote awareness of security best practices and current threats.
- Encourage a culture of security awareness and proactive threat identification.

2.7. Third-Party Management

- Assess the security practices of third-party vendors and partners.
- Implement contractual requirements for security measures and data protection.
- Monitor third-party compliance and conduct regular security audits.

2.8. Continuous Monitoring

- Implement continuous monitoring of systems for suspicious activities and anomalies.
- Utilize automated tools and systems for real-time threat detection.
- Regularly review and analyse security logs and alerts.

3. Research integrity considerations for WW4WL

Respecting to research integrity considerations by researchers is fundamental for advancing scientific knowledge, maintaining public trust, and ensuring the responsible conduct of research.

3.1. Honesty

- Apply accurate principles in collection, recording, and reporting of research data.
- Define a truthful representation of methods, results, and findings without fabrication, falsification, or misrepresentation.

3.2. Accountability

- Take responsibility for the validity and reliability of research actions.
- Participate to and respect the peer review process to uphold the quality and integrity of the research community.

3.3. Objectivity

- Ensure that personal or financial interests do not influence research outcomes.
- Provide transparency about potential conflicts of interest.

3.4. Transparency

- Provide clear and detailed descriptions of research methods to allow reproducibility.
- Make data available for verification and further research, where appropriate.

3.5. Respect for Intellectual Property

- Give credit to the work and ideas of others through appropriate citation and acknowledgment.
- Avoid the use of others' work without proper attribution.

3.6. Respect for Colleagues and Collaboration

- Foster a collaborative and respectful research environment.
- Create a fair and accurate representation of contributions to research projects.

3.7. Study protocol

- Define a comprehensive document outlining the plan of the research to conduct it systematically, ethically and efficiently (ANNEX 3).
- Protect both the users' (respondents) actions and the researchers by defining all actions (ANNEX 3).
- Describe all the partners and stakeholders involved, their roles and responsibilities (ANNEX 3).

3.8. Social Responsibility

- Consider the broader implications of research findings on society and the environment.
- Engage with the public and policymakers to inform and educate about research outcomes.

3.9. Rigorous Documentation

- Maintain thorough and accurate records of all research activities.
- Ensure the security and integrity of research data.

3.10. Adherence to Legal and Institutional Requirements

- Follow all relevant laws, regulations, and institutional policies governing research activities.
- Promptly report to any instances of research misconduct.

4. Support and training consideration for WW4WL

4.1. Practical Implementation

- Provide ongoing education on research integrity for all researchers.
- Create a culture of integrity through institutional policies, resources, and support systems.

4.2. Methodological Training

- Provide workshops on designing robust and rigorous research studies.
- Train researchers in various data collection methods relevant to their field.
- Offer courses on statistical analysis and data interpretation using software tools (e.g., SPSS, R, Python).

4.3. Data Management

- Train researchers in best practices for data management, including secure storage, data anonymisation, and archiving.
- Provide guidelines on responsible data sharing and collaboration.

4.4. Responsibility in Mentoring

- Provide appropriate supervision and support for junior researchers.
- Offer training in project management principles, including planning, scheduling, and resource allocation.
- Teach researchers how to set and track milestones and deliverables.
- Implement regular feedback sessions to help researchers improve their work.
- Conduct periodic performance evaluations to identify areas for improvement and provide support.

4.5. Security Awareness

- Provide regular training for all team members on data security best practices and protocols.
- Educate staff on recognizing and avoiding phishing attacks and other social engineering tactics.

ANNEX 2: Access control and role management

Access control and role management in a platform based on job or task profiles involves defining, assigning, and managing user permissions and access rights based on the specific responsibilities, tasks, and roles within an organization. This approach ensures that users have the appropriate level of access to perform their duties effectively, while also maintaining security and compliance.

The WW4WL project makes use of the MOTUS platform and the Delphi platform to collect data. Below per platform an oversight is given of how the platform is able to technically employ a role management strategy to ensure a high level of security. [The Delphi platform will be added in the next version].

1. MOTUS

The MOTUS data collection platform is used within the WW4WL project to collect data from employers and employees. The responsibility lies with the regional data collection teams, with for each team a Data Manager that oversees the necessary actions to design the studies, to collect the data and to download/process the datasets.

Study protocols support the employment of multiple data collection methods and strategies. These study protocols are developed prior to the data collection and provide a plan of the study protection both the respondent actions and the researchers together with all involved partners and stakeholders and the roles they are assigned.

In support of the Data Manager, MOTUS makes use of a Role-Based Access Control (RBAC). RBAC is an access control system principle that checks the assigned roles of every back-office-user/researcher and grants access to resources accordingly. This approach minimizes the risk of unauthorized access and ensures that back-office users only have access to the tools and data necessary for their tasks.

The validity in time of the access needs to be monitored by the Data Manager.

MOTUS is organised using 3 concepts:

1.1. Platform domain, Groups and studies

As a security concept the MOTUS data collection platform is installed as a cloud-based deployment on a hosted private server (VPS), operating independently with an own operating system, applications, and settings. The MOTUS data collection holds a front-office for respondents and a back-office for researchers.

The back-office is developed to design studies, to collect data, to monitor the fieldwork, and to process the data. The back-office is available as a web version with url:

https://backoffice.winwin4worklife.eu. Entering the back-office gives the availability to design and carry out different studies that are listed in a dashboard.

Studies are part of a Group. A Group serves as a level between the platform and the various studies. In this way studies from one Group are separated from studies from another Group. For the WW4WL project this means that every case study location (e.g. Luxemburg "Case study LU – Employers and Employees) has the availability over a Group holding the different studies like the surveys for employers and employees and the activity registration via time diaries and geotracking collected from the employees.

The data from the different case studies is separated and cannot be seen or downloaded by users from other Groups.

Back-office users are enrolled to a specific Group. Within a Group further access/restrictions to a study can be granted.

1.2. Platform administrator rights

For the WW4WL project the MOTUS data collection platform is hosted on the hbits environment (ISO27001). Platform administrator rights' respond to the highest level of permissions within a platform, granting the ability to manage and control all aspects of the system. This role has the ability to carry out:

- User and security management, involving the creating, modification, deletion of users, the assigning and managing of roles and password and authentication management.

  Within the WW4WL this role creates new users to the back-office. The platform administrator invites the new user to become part of a Group via an automated procedure. This procedure leads to the sending of an invitation email with a link. By clicking this link, the back-office user is able to provide a password (requirements apply) and to setup a 2FA procedure for secure entry to the platform.

  The platform administrator also assigns the role of Data Manager within each Group. A Data Manager holds all rights in a group and is able to manage the Group and to create, adapt and delete studies.

- System configuration, involving platform settings and integration with other systems (like the geolocation microservice).

- System maintenance, involving software updates, performance optimisation, troubleshooting and support.

- Environment management, involving production and development environments, and control the deployment strategy.

As the Platform administrator moreover has technical rights, this role can be exempted from entry to studies created in the Group. This means:

- Possible exclusion of entry to studies by the Data Manager by granting exclusive rights to Study consultants (or only to themselves).

1.3. Data Manager and study consultant role

A Data Manger or study consultant is linked to only one Group hosted at the MOTUS data collection platform (operating under the same domain). The Platform administrator invites a user to a Group with the option to:

- Login (default)
- Create and copy studies
- Access extra group features (eg. all respondents, username generators, meta-data collection)

The invitation procedure is automated, where a new user receives an email invitation to join a Group. In the first step, the user is prompted to set up a username (email address) and password. In the second step, MOTUS requires the user to configure a 2FA entry using an authentication app, which provides a one-time login code for accessing the MOTUS data collection platform.

A Data Manager holds all three options, most users will only hold the option to log in to the back-office and are considered Study consultants.

Once a Study consultant is enrolled to a Group a Data Manager can further define the user rights of this user. User rights can be defined per different study within the same Group.

In total 18 different rights (not all are relevant to WW4WL) can be added to a Study consultant within a study:

<u>Overall -</u>

- Manage study team
  Provides the right to define which users can access the study. This right is usually only given to a Data Manager.
- Configure and delete the study
  Set name, start/end date, description, draft/active/pause/finish

<u>Study components -</u>

- Edit surveys
  Create and edit surveys
- Edit diaries
  Create and edit diaries
- Edit communication
  Create and edit communication (page, mail, notification)

- Edit classifications (not for WW4WL)
  Create and edit COICOP lists
- Edit group (not for WW4WL)
  Create and edit groups (of respondents)
- Translate study components
  Set default language and translate to secondary languages

Study setup -

- Edit the study flow
  Create and edit respondent journey
- Manage communication preferences
  Configure settings, emails and pages
- View flow statistics
- View study results

Respondents –

- Import respondents
  Add new respondents to a study
- Manage respondents
  Define a username, password requirements
- Delete respondents
  Remove respondents
- Manage respondent preferences
- Manage merge fields
  Add information at import to respondents

Data –

- Export all respondent data
  Download data as a JSON file

Important note:

As long as no user is linked to a particular study, all users have full access rights to that study.

2. KoboToolbox plataform

KoboToolbox is a widely used digital platform for survey-based data collection, particularly well-suited to research and humanitarian projects. Within the WW4WL project, KoboToolbox is used to collect structured survey data from digital nomads case study, conducted in Lisbon, Portugal. The implementation and management of the survey through KoboToolbox is carried out by the regional data collection team of Portugal, the IST-ID team, which has a designated Data Manager. This person is responsible for organizing the survey, managing the data collection process, and

overseeing the downloading and processing of datasets once responses have been gathered, under the supervision of IST-ID research responsible (KoboToolbox, 2025b).

Study protocols support the employment of multiple data collection methods and strategies. These study protocols are developed prior to the data collection and provide a plan of the study protection both the respondent actions and the researchers together with all involved partners and stakeholders and the roles they are assigned.

In support of the Data Manager, the research team makes use of a Role-Based Access Control (RBAC). RBAC is an access control system principle that checks the assigned roles of every back-office-user/researcher and grants access to resources accordingly. This approach minimizes the risk of unauthorized access and ensures that back-office users only have access to the tools and data necessary for their tasks. The validity in time of the access needs to be monitored by the Data Manager (KoboToolbox, 2025e).

Here, we can also organize KoboToolbox information using 3 concepts:

2.1. Platform domain, Groups and studies

KoboToolbox is a web-based data collection platform accessed at the domain: https://eu.kobotoolbox.org. KoboToolbox's European server ensures that data is stored exclusively on servers located in Europe, in compliance with the GDPR. KoboToolbox is deployed as a cloud-based solution with the option for organizations to self-host for greater control over data sovereignty and security. Its scalable infrastructure enables teams of all sizes to deploy data collection projects efficiently and securely (KoboToolbox, 2025b).

The KoboToolbox data collection features a separate interface for respondents and researchers. The front end includes the tools with which users interact to complete forms, whether via the KoboCollect mobile app or through the web-based format accessible on browsers. In that case, the responders can log in or create a new account when solicited, through the app or the link available for the survey (KoboToolbox, 2025i).

The back end consists of the project management console, where users design forms, manage projects, monitor incoming data, and export datasets. It is developed to design studies, to collect data, to monitor the fieldwork, and to process the data. The back-office is available as a web version with url: https://www.kobotoolbox.org/sign-up/. Entering the back office gives the availability to design and carry out different studies that are listed in a dashboard of projects (KoboToolbox, 2025b).

In KoboToolbox, data and access are organized at the Project level. Each project corresponds to a specific study and contains the collection forms (questionnaires, diaries, etc.). There is no formal concept of Group as in MOTUS, but it is possible to simulate this structure through the use of Collections, where different projects can be grouped for a specific unit of analysis or location. Each project works in isolation, with access permissions assigned individually. Thus, data from one project cannot be

viewed or downloaded by users from another project, unless explicit sharing is done (KoboToolbox, 2025e).

2.2. Platform administrator rights

For the WW4WL project the KoboToolbox data collection platform is hosted in a UE server, located in Ireland. The administration of the KoboToolbox infrastructure on the European server is carried out by the technical team responsible for the platform, which ensures the maintenance of the servers, the application of updates, the security of the infrastructure and the smooth running of the environment (KoboToolbox, 2025b). This team does not interfere with the content or configuration of projects created by users. They have the ability to carry out:

- Environment management: server maintenance, system updates, infrastructure security and platform availability.
- System maintenance: application of updates, performance optimization, technical support.
- System configuration, involving platform settings and integration with other systems.

At the project level, the most privileged role falls to the Project Administrator, who has full powers over the management of forms, access permissions and data export. The Project Administrator defines the roles of other users – such as editors, data viewers or just collectors – by sharing the project with their emails. They are responsible for the survey, managing access, configuring the project's security settings and ensuring the use of good practices.

Here, the questionnaire administrator can invite other researchers and manage their access to the available data and resources, such as making the questionnaire available and any changes to its structure. This procedure leads to the sending of an invitation email with a link. By clicking this link, the research user is able to create their own account and to setup a 2FA procedure for secure entry to the platform.

This administrator also assigns the role of Data Manager. A Data Manager holds all rights and is able to manage the survey and to create, adapt and delete fully the project. At project level, the Project Administrators (designated in KoboToolbox) have the highest level of permissions. They are responsible for:

- Project user management: creating permissions, sharing projects, defining roles (Admin, Editor, Data viewer, Collection only).
- Project management: creating, editing and deleting forms; configuring project parameters; exporting data; controlling who can access or edit the project.
- Invite users: the Project Administrator shares the project with other users via email, assigning the appropriate role.
- Security configuration: recommendation to use strong passwords and enable 2FA at the user account level.

2.3. Data Manager and study consultant role

A Data Manger or study consultant is linked to the case study of digital nomads, hosted at the KoboToolbox data collection platform (operating under the European server). The Platform administrator invites a user to a project with the option to:

- Login (default).
- Create and copy studies.
- Access extra group features (e.g. all respondents, meta-data collection).

The invitation procedure is done manually, where a new user receives an email invitation to join a project, sent by the project manager. The invited user receives a link to access the project with the assigned permissions (KoboToolbox, 2025j). In the first step, the user is prompted to set up a username (email address) and password, based in the EU or global server. In the second step, it can be required to the user to configure a 2FA entry using an authentication app, which provides a one-time login code for accessing the data collection platform.

In KoboToolbox, the role equivalent to the Data Manager is the Project Administrator. This user has full control over the project and its settings. They:

- Creates and manages forms (questionnaires, diaries, etc.).
- Defines which other users there will be access to the project and at what level (Editor, Data Viewer, Collection Only).
- Ensures compliance with data protection regulations, including the periodic review of access.
- Exports and manages the data collected.

The role equivalent to Study consultant in MOTUS is the user with Editor or Data viewer permissions in KoboToolbox:

- Editor: can edit forms and view data, but cannot change other users' permissions.
- Data viewer: can only view and export data, without editing forms or settings.
- Data collector: can only send data, without access to the content of the data collected or the design of the project.

There are different rights (not all are relevant to WW4WL) can be added to a manager within a project:

<u>Overall -</u>

- Manage study team
  Provides the right to define which users can access the study. This right is usually only given to a Data Manager.
- Configure and delete the study
  Set name, start/end date, description, draft/active/pause/finish.

Study components -

- Edit surveys and projects
  Create and edit surveys and other projects.
- Translate study components
  Set default language and translate to secondary languages.

Study setup -

- View project statistics.
- View study results.

Respondents –

- Delete respondents
  Remove respondents.
- Manage respondents' data
  View respondents' answers.

Data –

- Export all respondent data
  Download data as a CVS, XLS, or GeoJSON file.

Important note:

In KoboToolbox, by default, only users explicitly invited to a project have access to it. This means that a project created by a user remains private until it is shared. The project administrator must manage these accesses diligently to ensure data security and privacy.

3. Delphi platform

To be included later.

ANNEX 3: Template Study Protocol

A Study Protocol is a document that describes the background, rationale, objective(s), design, methodology, statistical considerations and organisation of a data collection. By having so, a study protocol is a binding document to ensure safety of personal data.

Key words:

- Sensitive & personal data
- Multiple contact (moments)
- Different roles
- Cross boarder

Roles:

- Principal Investigator
- Data Manager
- DPO
- Ethics Manager
- Institutional Ethics Committees
- WW4WL ethics board
- Researchers
- Data Subjects

1. General information

2. Rationale & Background information

3. Study Objectives

4. Study Design

5. Methodology

6. Safety Considerations

7. Follow-up

8. Data Management and Statistical Analysis

9. Quality Assurance

10. Expected Outcomes of the Study

11. Dissemination of the Results and Publication Policy

12. Duration of the Project

13. Anticipated Problems

14. Project Management

15. Ethics

16. Budget

17. Supplementary Support for the Project

18. Collaboration With Other Researchers or Institutions

19. Curriculum Vitae of All Investigators

20. Other Research Activities of Investigators

21. References

ANNEX 4: Data incident and recovery plan

An Incident Response Plan (IRP) is a coordinated strategy for handling and responding to security breaches or cyberattacks. Its goal is to minimize harm, shorten recovery time, and reduce the risk of future incidents.

1. Security breach

A security breach happens when personal data has been lost, or there has been unlawful processing (security incident). This happens when there is:

- A destruction or loss of personal data
  E.g.: Data centre fire, accidental deletion of a file without backup
- Damage, unauthorized access, incorrect provision
  E.g.: Loss of USB stick, stolen laptop, malware, hack, email to wrong recipient

2. Breach management

The following actions apply to prevent incidents

- Automated check for hack, malware, …
- Implement security tools (firewalls, encryption, …) and infrastructure (certifications, entrance, …) that are up-to-date and monitored
- Reporting every internal incident to a fixed contact person
- Creation of internal procedures and training/awareness
- Assemble a response team involving members from different departments (IT, legal, communication, …)
- Agreements on reporting external security incidents

To this end a registration form and a key personal contact list is available. This also includes a list of external contacts if necessary.

3. Breach investigation

The following questions apply to get a full picture of the security breach:

- Description of what exactly has happened to the data
- Description of the nature of the personal data affected
  E.g.: Special data, personal data of sensitive nature
- Description of the extent of the incident
  E.g.: Number of people affected, amount of data affected per person, is the affected data shared within a chain?
- Description of the category of persons affected

E.g. Respondents, employees, clients, market contacts
- Description on the impact on those affected
  E.g. Vulnerable groups, financial loss, material/immaterial damage

4. Breach repairing

Breach repairing involves the steps taken to restore and secure an organization's systems and data after a security breach has occurred. The process is crucial to ensuring that the breach's impact is minimized and that similar incidents are prevented in the future

4.1. Measures to limit the consequences of the incident

The flowing measures apply:

- Reporting to the DPO and the Authority for the Protection of Personal Data.
- The persons affected by the data breach must be informed if the security breach is likely to have an adverse effect on their privacy.
- Inform affected persons on how to protect themselves to this infringement.

In case of negative consequences for the affected persons a report has to be done within 72 hours after the security breach to the Authority for the Protection of Personal Data and the DPO.

Measures also involves communication to the outside world if necessary. It also involves the coverage for third-party liability, own costs, and possible fines.

4.2. Prevent similar incidents in the future

Prevention measures apply:

- Plan updating
- Plan documentation storage
- Improve backup strategy
- Renew risk management
- Document triggering events
- Plan emergency response team