Funded by
the European Union

ROBOtics KNOwledge Transfer Lab Project

ROBO-KNOT

GA: 101216484

Data Management Plan

Deliverable D4.3

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 European Research Executive Agency can be held responsible for them.

Deliverable D4.3 Data Management Plan

Work package	**WP4 PROJECT MANAGEMENT AND COORDINATION**
Task	Task 4.3 Data management and monitoring of legal and ethical aspects
Due date	28-02-2026
Submission date	27-02-2026
Deliverable lead	EIT Digital Hungary
Version	V1.0
Authors	Marton Belik (EITDH), Gergely Horváth (EITDH), Krisztián Gál (EITDH)
Reviewers	Efstratios Stylianidis (AUTH), Alba Domínguez Pedreira (CTAG)

Abstract:

The ROBO-KNOT Data Management Plan (D4.3) defines the project's strategy for handling research, administrative, and dissemination data throughout the project lifecycle. It identifies the main categories of data processed within the project, including internal management documentation, secondment-related information, training outputs, and public dissemination materials. The plan ensures alignment with the FAIR data principles, while safeguarding sensitive and personal data in compliance with EU regulations.

Document revision history

Version	Date	Description of change	Contributor(s)
V 0.1	16-02-2026	1st version of deliverable template shared with partners.	Marton Belik (EITDH)
V 0.2	19-02-2026	Partners provide input	Michal Rybacki (ADRA), Ottavia Migliavacca (ADRA), Efstratios Stylianidis (AUTH), Ioannis Tavantzis (AUTH), Eleni Karachaliou (AUTH), Ifigeneia Skalidi (AUTH), Anna Dosiou (AUTH), Alba Dominguez Pedreira (CTAG), Matteo Falsetta (EITD), Jan Babic (JSI), Annela Hendrikson (TALT), Tõnis Segerkrantz (TALT), Ingrid Hunt (TSP), Ricardo Sobral (PACT), Ghadir Hummeid (ULUS)
v0.3	24-02-2026	WPLs provide (final) input	Ifigeneia Skalidi (AUTH), Matteo Falsetta (EITD), Michal Rybacki (ADRA), Marton Belik (EITDH)
V 0.4	25-02-2026	Reviewed by	Efstratios Stylianidis (AUTH), Alba Domínguez Pedreira (CTAG)

v.1.0	27-02-2026	Approved by the coordinator	Marton Belik (EITDH), Krisztián Gál (EITDH)

Nature of the deliverable	**to specify: R**
Dissemination level	
Public - fully open. e.g., website	**PU**

Table of Contents

Abbreviations 5

1. Executive Summary 6

2. Introductions 6

2.1. ROBO-KNOT project 6
2.2. Work Package 4 (WP4) 7
2.3. Data Management Plan (D4.3) 7

3. Data summary 8

3.1. Purposes for data collection: 8
3.2. Data Mapping 9
3.2.1. Data categories 9
3.2.2. Personal data collected from secondees: 10
3.2.3. Legal basis of processing personal data, privacy statement(s) 11
3.3. Personal data shared with third parties 12
3.4. Deliverables and Milestones: 13

4. Data Security 14

4.1. Exchange of Data During Development Phase 14
4.2. Database Safety and Security 14
4.2.1. Core Microsoft Cloud Security Components: 15
4.2.2. Third party IT tools 15
4.3. Data retention periods, destruction of data 16
4.4. ROBO-KNOT Joint Controllership Agreement (RK JCA) 16

5. Risk assessment 18

6. Ethics 19

6.1. FAIR Data Principles 19
6.2. GDPR 20
6.3. Gender balance monitoring 20
6.4. Individuals' rights 20
6.5. Contact information 21

7. Revisions of the ROBO-KNOT Data Management Plan D4.3 21

Abbreviations

CNAPP	Cloud Native Application Protection Platform
DLP	Data Loss Prevention
DPAs	Data Protection Authorities
DPO	Data Protection Officer
EC	European Commission
EC PO	European Commission Project Officer
EIT	European Institute of Innovation and Technology
ERA	European Research Area
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
GEA	General Assembly
HE	Horizon Europe
KPI(s)	Key Performance Indicator(s)
NAIH	Hungarian National Authority for Data Protection and F
OLAF	European Anti-Fraud Office
PC	Project Coordinator
PCDP	Personal Career Development Plan
PEC	Project Executive Committee
QM	Quality Manager
R&I support staff	Research & Innovation support staff
RBAC	Role-Based-Access Control
RK JCA	ROBO-KNOT Joint Controllership Agreement
TL	Task Leader
TSC	Talent Selection Committee
WPL	Work Package Leader

1. Executive Summary

This **Data Management Plan D4.3 (DMP)** defines the procedures, standards, and responsibilities governing the collection, processing, storage, sharing, protection, and long-term preservation of data generated within the ROBO-KNOT project. The document ensures that project data management follows the FAIR principles—Findable, Accessible, Interoperable, and Reusable—while fully complying with GDPR, ethical requirements, and Horizon Europe regulations.

ROBO-KNOT generates multiple categories of data, including:

- administrative and project management documentation,
- secondment-related personal and institutional data,
- training and skills-development materials,
- monitoring, evaluation, and quality assurance data,
- dissemination and communication outputs.

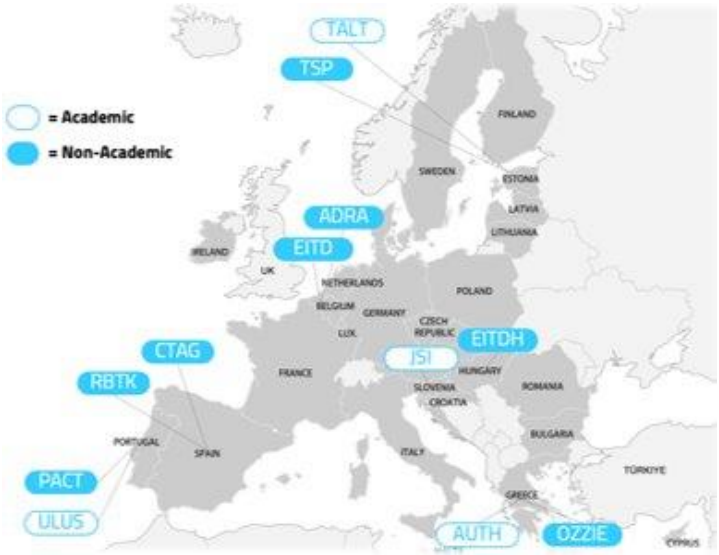
The DMP establishes governance mechanisms, security measures, access rules, and update procedures to guarantee secure handling of sensitive information and open dissemination of non-confidential results, thereby supporting transparency, compliance, and long-term impact.

This Data Management Plan (D4.3) serves as a supplementary document to be used alongside the Project Management Plan (D4.1) and the Quality Manual (D4.2), which provide further operational and procedural details.

2. Introductions

2.1. ROBO-KNOT project

The ROBOtics KNOwledge Transfer Lab (ROBO-KNOT) is a cross-sectoral and cross-border mobility initiative designed to accelerate knowledge transfer in the Robotics field. By facilitating secondments of Research and Innovation (R&I) talent between academic and non-academic sectors, this project aims to promote more attractive and sustainable research careers in Widening Countries, in alignment with the European Commission's ERA Policy Agenda (Action 4). The project will directly involve 24 researchers and 12 R&I support staff from academic



institutions in Widening Countries (Greece, Portugal, Slovenia), who will be seconded to non-academic organisations in either Widening (Estonia, Greece, Portugal) or non-Widening (Spain) countries. ROBO-KNOT's structured methodology, comprising Pre-secondment, Secondment, and Post-secondment phases, ensures impactful skills development and knowledge exchange. Firstly, talent is carefully selected and matched with opportunities that align with both individual goals and hosting organisations' strategic needs. Through a modular secondment approach, participants are then immersed in diverse work settings, enhancing their practical knowledge of Robotics technologies' commercial development. Finally, the Post-secondment phase includes targeted training activities and ongoing support to ensure long-term impact of the action, particularly with regards to the innovation-to-commercialisation pipeline. ROBO-KNOT aims to develop a tailored Skills Development Framework, in line with the European Commission's ResearchComp, as well as a Career Advancement Plan, which ensures high impact of the project on secondees' employability, future career prospects and knowledge sharing capabilities. ROBO-KNOT not only benefits seconded talent individually, but also increases consortium organisations' R&I support capacity and ability to establish effective cross-sectoral and cross-border collaborations, contributing to a more integrated European innovation ecosystem.

2.2. Work Package 4 (WP4)

Work Package 4 (WP4) in is dedicated to comprehensive management of the ROBO-KNOT project, encompassing operational, administrative, and financial oversight. It ensures effective coordination across consortium partners through structured communication and regular engagement, fostering long-term collaboration. WP4 implements rigorous quality assurance and risk management protocols, while ensuring compliance with ethical, legal, and gender equality standards, including robust data management practices. These measures collectively support the delivery of project objectives on time and within budget.

The deliverables of WP4 are:

- D4.1 – Project Management Plan, M3
- D4.2 – Quality Manual, M5
- D4.3 – Data Management Plan, M6

2.3. Data Management Plan (D4.3)

ROBO-KNOT is a HORIZON Coordination and Support Action, and therefore it does not generate robust research data or scientific datasets typically associated with R&I-focused Horizon Europe actions. Instead, the project primarily produces administrative, management, mobility, training, and communication-related data, all of which remain document-based and moderate in volume. However, because the project processes significant amounts of personal data—including application files, secondee

documentation, training records, and communication materials—it must still meet strict data-management and data-protection obligations.

The purpose of this Data Management Plan is to define the procedures and standards governing how data generated and processed within the ROBO-KNOT project are collected, documented, stored, protected, shared, and preserved throughout the project lifecycle. It describes the types of data involved, establishes rules for secure handling and controlled access, and ensures full compliance with legal, ethical, and regulatory requirements, including GDPR and Horizon Europe obligations. The plan also supports the application of open science practices and the reuse of non-confidential results where appropriate, while clearly assigning roles and responsibilities for transparent, accountable, and efficient data governance across the consortium.

3. Data summary

ROBO-KNOT project (the data collector) commits to protecting personal data and respecting Privacy of individuals, by collecting and further processing personal data pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

3.1. Purposes for data collection:

The purpose of data collection is to support, project implementation and coordination, to monitor progress and KPIs, to follow-up on capacity building and training evaluation, to support evidence-based policy making and dissemination outputs, and to meet audit and compliance requirements. To achieve the above objectives, personal data may be collected and processed for the following activities and purposes:

- to organize, implement and put in place all the activities, events and actions regarding the ROBO-KNOT project,
- to process and facilitate secondee application, selection, management and follow-up, and access requirements to the above-mentioned project,
- to protect secondees' health and safety,
- to monitor and evaluate the secondees' progress,
- to attribute the eventual provisions by sending institutions (AUTH, JSI, ULUS),
- for mobility opportunities and management,
- for statistical purposes,
- to audit and report to the EC, EIT and European bodies,
- for dissemination of information and the communicational purposes,
- and other legitimate and lawful reasons which are compatible with the above.

3.2. Data Mapping

3.2.1. Data categories

ROBO-KNOT processes several categories of data:

1. **Administrative and management data:**
   Description: This category includes documents and records that support the internal coordination, governance, monitoring, KPI tracking and reporting functions of the consortium. Examples include project deliverables and milestones, meeting minutes, governance documents, internal reporting, and interim and final reporting and KPI tracking files.
   Type of data: reports, deliverables, minutes, governance documentation, internal monitoring, financial and personnel reporting data, KPI tracking.
   Data Format: contact lists(s) (.xlsx/.csv), meeting agenda(s), minutes of the meeting, meeting recordings (.docx/.pdf/.pptx/ .mp4), project progress tracking (.xlsx/.csv), and reporting files (.docx/.pdf/.pptx/.xlsx/.csv).

2. **Secondment-related** (**including training and capacity-building) data**
   Description: A substantial portion of the project's data relates to the management of secondments and associated training activities. These datasets originate from applicants, secondees, host organisations, and training providers. They include application forms, CVs, eligibility and institutional confirmations, endorsement letters, personal development records, mobility agreements, follow-up, reporting and evaluation forms, and documentation linked to structured post-secondment activities (training programmes) such as the SPIN modules or Bootcamps.
   Type of data: submitted application materials, CVs, eligibility verification, institutional (sending, host) confirmations, mobility mentoring and evaluation forms; and SPIN training materials, Robotics Commercialisation Bootcamp(s) and Innovation Leadership Bootcamp, learning outputs, learning assessment feedback).
   Data Format: applications register (.xlsx/.csv), application files (.pdf), archive of applicants' correspondence (.pdf), secondees register (.xlsx/.csv), secondee post-secondment activity performance register (.xlsx/.csv), archive of secondees' correspondence (.pdf)., training materials (.docx, .xlsx/.csv, .pdf).

3. **Dissemination and communication outputs** (public events (e.g. info session).
   Description: This category covers internally and publicly oriented materials produced to promote project activities and communicate results. Examples include presentation slides, event documentation (such as info sessions), public deliverables, publications, outreach analytics, and stakeholder engagement

data. These materials are typically non-sensitive and published openly on the project website or used in external digital platforms such as LinkedIn or YouTube.
Type of data: event materials and presentations, deliverables, publications, outreach metrics and stakeholder engagement data.
Data Format: event register (.xlsx/.csv), event materials (.docx, .pptx, .pdfx), outreach metrics monitoring materials (.xlsx/.csv.docx, .pptx, .pdfx).

These datasets originate from project partners, participants, and project coordination activities.

Due to the nature of the data, personal data is GDPR protected. Data volumes are expected to remain **moderate and document-based**, typical of Coordination and Support Actions, without large experimental datasets, and processing of any data will take place on a legitimate basis in accordance with to Art. 6 Regulation (EU) 2016/679 (GDPR).

3.2.2. Personal data collected from secondees:

At the (event) registration stage, the following personal data will be collected and processed:

- Registries' personal data, such as name, surname, e-mail

At the application stage, the following personal data will be collected and processed:

- Applicants' personal data, such as name, surname, date of birth, gender, nationality, country of residence, address, e-mail, phone numbers, current employment institution, education, employment, activities, memberships etc.
- Name of the PhD supervisor, institutional head or line manager
- Endorsement letter from PhD supervisor, institutional head or line manager as provided by the applicant
- English proficiency certificates
- Curriculum Vitae including details of academic and professional career
- Letters of motivation
- Copies of relevant. Certificates or proof of employment

After the participants' successful application, the following personal data will be collected and processed:

- ROBO-KNOT project program and course ROBO-KNOT post secondment activity notes, results and all other facts that are necessary to evaluate the participant's performance,
- Attendance records or absence of the participant and any personal information justifying the absence,

- Video, audio and photo of the participants taken during their participation to the programme activities and events and other recording taken during their time of the secondment (for instance video and written interviews, text for success stories, students info included into newsletter, etc.),
- All information about the mobility and training activities, such as contract with the company, letter of engagement, three-party agreement etc., and the final deliverables of the mobility such as reports, Personal Development Plan updates, monthly reports and the final report etc.,
- Any other information pertinent to the organization, implementation or reporting needed for EITDH, ROBO-KNOT project and the obligations that ROBO-KNOT project and EITDH or other project partners might have in terms of audit, reporting, work implementation and accountability towards EU and EIT and the partners of the project.
- Registration in and results of the attended ROBO-KNOT project.
- Registration to and achievement of international, intersectoral mobility.
- Registration to and achievement of cross-organizational mobility.
- Responses to surveys and competitions.
- Any special requirements or points of interest participants indicate during the registration to events.

3.2.3. Legal basis of processing personal data, privacy statement(s)

This privacy statement(s) of ROBO-KNOT project explains the reason for the processing of personal data in the context of actions for the ROBO-KNOT project. Privacy statements explain the way ROBO-KNOT project collects, handles and ensures protection of all personal data provided, how that information is used and what rights an individual has in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the competent national data protection authorities (DPAs).

3.2.3.1. Consent of the data subject:

At the registration/application phase, by filling and/or submitting the application form, applicants give their consents according to which their personal data can be collected and be processed by the EIT Digital and its organizations based on Article 6 paragraph 1(a) of the GDPR. The data controllers need to assess the applications in order to offer a place in the framework of the ROBO-KNOT project.

3.2.3.2. Contractual base

When individuals are a participant of ROBO-KNOT project:

When processing personal data is necessary for the performance of a contract to which the data subject is party, Article 6 paragraph 1(b) GDPR is the legal basis for the processing. Indeed, the data controllers need to process personal data, in order to

organize, manage, implement, follow-up and promote ROBO-KNOT project (including web-streaming, photos, audio-visual recording) based on the contracts individuals have signed. This also applies to processing operations that are necessary in order to take steps prior to entering into the contract.

Below are the contracts that might concern our participants depending on their case:

- ROBO-KNOT three party secondee agreement

3.2.3.3. Compliance with a legal obligation

EIT Digital Hungary and its partners will collect and process personal data when it is required for compliance with a legal obligation to which the data controllers are subject and Article 6 paragraph 1(c) GDPR is the legal basis for this processing. These legal obligations are listed as follows:

- Legal obligation laid down by ROBO-KNOT project(?), EU, EIT Regulation including the legal obligation of reporting to the EU and EIT,
- Legal obligation laid down by Horizon Europe Regulation, including the legal obligation of disseminating and communicating information regarding HE funded activities,
- And other national, European and international binding regulations.

3.3. Personal data shared with third parties

Access to personal data is provided to EITDH and ROBO-KNOT project partners staff responsible for carrying out this processing operation and to other EIT Digital Hungary and ROBO-KNOT project partners staff according to the “need to know” principle.

- The controllers will exchange with each other, the personal data mentioned in this statement or signed contract.
- All personal data collected by the data controllers will be also transferred and stored on the SharedRepository of EITDH in accordance with legal obligation imposed on the data controllers.
- The data controllers may collect and exchange the personal data of students with NOT-Academic organizations, companies, startups or research centers for the mobility. The sharing of your information with the programme partners (Universities etc.), the Talent Selection Committee (TSC) responsible for the secondee’s selection, EU, EIT, entities participating in the mobility actions and service providers for the programme.
- The data controllers may share the personal data of the students where it is required by applicable regulation with the following organizations: the EU, EIT, the Court of Auditors, OLAF, the European Ombudsman, the European Data Protection Supervisor, the General Court and the European Court of Justice.

3.4. Deliverables and Milestones:

Amongst project output are the thirteen Deliverables and eleven Milesones, of the thirteen Deliverables two deliverables are sensitive.

D1.1, Open call for applications (PU), ***D1.2, First report on secondments (SEN), D1.3, Second report on secondments (SEN)***, D2.1, Career Advancement Plan – Handbook (PU), D2.2, Report on post-secondment skills development for R&I support staff (PU). D2.3, Report on post-secondment skills development for researchers (PU), D3.1, D&E&C Plan (PU), D3.2, Interim report on D&E&C activities (PU), D3.3, Executive report, including case studies and policy recommendations, on R&I secondments for knowledge valorisation (PU), D3.4, Final report on D&E&C activities (PU), D4., Project Management Plan (PU), D4.2, Quality Manual (PU), D4.3, Data Management Plan (PU).

3.4.1. Sensitive deliverables

ROBO-KNOT project operates with two sensitive deliverables (WP1, D1.2 - First report on secondments (due M12) and D1.3 - Second report on secondments (due M27)). Sensitive deliverables relate to materials that contain personal, and strategically relevant information whose disclosure could affect individuals, partner organisations, or the integrity of project implementation. In all cases, project materials will align with the FAIR data principles and GDPR, where needed, personal data will be secured and anonymised.

The data of the two sensitive deliverables includes secondment application files and lists, eligibility verification records, CVs, evaluation and selection documentation, mobility monitoring forms, and any internal assessment of participants' performance or career development.

Access to sensitive deliverables is strictly limited to authorised consortium members (PC and WP1) on a need-to-know basis and is managed through secure repositories with role-based permissions, version control, and traceable document handling.

All processing of personal data follows GDPR principles, including data minimisation, purpose limitation, anonymisation of data, secure storage, and defined retention periods. Where required, confidentiality obligations established in the ROBO-KNOT Consortium Agreement, and the Joint Controllership Agreement governs the handling and sharing of such information, ensuring that sensitive data are protected throughout the project lifecycle and beyond.

3.4.2. Public deliverables

ROBO-KNOT project will also prepare eleven public deliverables, of which, two are rooted in the personal data and progress data of secondees, such as D2.2 Report on post-secondment skills development for R&I support staff, and D2.3 Report on post-secondment skills development for researchers. In these two cases, project materials

will align with the FAIR data principles and GDPR, where needed, personal data will be secured and anonymised.

Public deliverables address applicants, stakeholders, and decision makers, and will be publicly available on the project's website.

The deliverable resulting collecting personal data is the D1.1 Open Call for Applications and it was published on the project's website and supports Open Science through transparent access, equal opportunity, and clear public documentation of eligibility rules, selection steps, and key timelines. Where appropriate, WP1 also makes available public templates and guidance (e.g., application form structure, general evaluation criteria descriptions, process overview) to support transparency and reproducibility of the selection process. The operational workflow and tooling are designed for traceability and GDPR-compliant handling.

Further public deliverables, such as the ROBO-KNOT Project Management Plan (D4.1 due by M3) describes organizing day to day work, and ensures efficient collaboration, traceability of project outputs. "Part 6. Organizing day to day work" describes the secure work in the SharedRespository, online-tools, "Part 6.2 the File naming Convention", "Part 6.4 the Version Control" and Part 8 describes the "Preparation of Deliverables and Milestones."

4. Data Security

4.1. Exchange of Data During Development Phase

During the development and implementation of the ROBO-KNOT project, data exchange among consortium partners is conducted through secure, access-controlled digital collaboration environment. Partners use institutionally approved accesses (institutional Microsoft accesses) to connect to the collaboration platform and shared repository (Microsoft SharePoint and Teams) of the project. This ensures authenticated user access, role-based permissions, and traceability of document handling. Sensitive or personal data are shared only when strictly necessary and in accordance with the project's data protection and the ROBO-KNOT Joint Controllership Arrangement.

Access rights are granted following the principle of least privilege and are regularly reviewed by responsible project and institutional representatives.

4.2. Database Safety and Security

All project-related databases and structured data repositories within ROBO-KNOT are hosted on secure institutional infrastructures (Microsoft Data Cloud Security) managed by consortium partners in accordance with their internal IT governance frameworks and EU data protection requirements. These environments rely on protected servers with

controlled physical and logical access, regularly updated security configurations, and firewall protection to prevent unauthorised intrusion or data leakage.

To ensure and prevent data loss, the PC implements routine backup procedures, every 6 months, including versioned backups. Redundancy mechanisms and recovery protocols are maintained in line with institutional disaster-recovery policies, ensuring that project data remain available and restorable throughout the project lifecycle.

Data integrity is safeguarded through controlled editing rights, audit trails, and periodic monitoring of stored information. Any anomalies, corruption risks, or security incidents are handled according to institutional security procedures and the project's governance framework.

4.2.1. Core Microsoft Cloud Security Components:

- **Encryption:** Data is encrypted at rest and in transit using industry-standard protocols, including two or more independent layers of encryption.
- **Identity & Access Management:** Role-based access control (RBAC) and strict, limited access for Microsoft personnel ensure that only authorized users manage data.
- **Microsoft Defender for Cloud:** A cloud-native application protection platform (CNAPP) that offers security across hybrid and multi-cloud environments, providing workload protection and security posture management.
- **Threat Protection & Recovery:** Microsoft 365 includes ransomware detection, automatic alerts, and file recovery capabilities (up to 30 days).
- **Compliance & Governance:** Features sensitive information labels, data loss prevention (DLP), and compliance with global privacy standards.

4.2.2. Third party IT tools

ROBO-KNOT uses third party IT tool(s) to inform about and promote events through widely used communication channel(s), including the social media via our pages on LinkedIn and YouTube. Should any platform become obsolete, or ROBO-KNOT accounts be discontinued for any reason, this will be communicated and updated on our website.

The use of third-party IT tools to connect to those services might set cookies when our website pages are loaded on your computer (or other devices).

These third-party services are provided by different entities not affiliated with the PC and its' project partners, and have their own terms of service and privacy policies. The use of a third-party IT tool does not in any way imply that PC or ROBO-KNOT project endorses them or their privacy policies.

In the event that one or more third party IT tools are occasionally unavailable, we accept no responsibility for lack of service due to their downtime.

4.3. Data retention periods, destruction of data

The Data Controllers only keeps personal data for the time necessary to fulfil the purpose of collection or further processing. Once the purpose of the collection is addressed, the data will be archived by the PC and removed securely from the active base. All personal data collected will be anonymised upon completion of the project.

The Data Controller will retain the personal data in its archive for a period up to January 2029 and after this period, the personal data will be anonymized. Annex 1: Description of Personal Data Processing Activities of ROBO-KNOT Joint Controllership Agreement provides a detailed description of project activity, joint controllers involved, purpose of processing, lawful basis of the processing, means of processing, categories of personal data and categories of data subject and „other information" including roles and responsibilities of parties, receipient of the data sets and their retention periods.

4.4. ROBO-KNOT Joint Controllership Agreement (RK JCA)

The ROBO-KNOT project is (also) an EU-funded mobility and knowledge-transfer programme focused on robotics. It involves secondments of researchers and R&I support staff. Execution of the project requires processing personal data; the parties jointly determine means and purposes, therefore falling under GDPR joint controllership. Each organisation is legally represented by authorised signatories.

The Agreement governs joint controllership obligations, roles, responsibilities, and cooperation mechanisms and it is effective until all joint processing activities end.

The Agreement lists roles, responsibilities and cooperation, and as general principles Joint Controllers must:

- Cooperate in fulfilling GDPR obligations.
- Process personal data only as specified in Annex 1.
- Restrict access to authorized persons only.
- Implement technical and organizational security measures per Art. 32 GDPR.
- Use processors only in compliance with Art. 28 GDPR.
- Keep all processing within the EEA.
- Allow audits and share compliance documentation.

Each Joint Controller is involved differently depending on the processing activity, as detailed extensively in Annex 1 (contact forms, applications, event registrations, training, communication activities).

Upon a request of a Data Subject Joint Controllers must:

Take the lead when they receive a request, or transfer lead responsibility if justified.

Notify all other Joint Controllers of every request, including:

- Request description
- Actions taken
- Proposed response
- Assistance requested
- Confirmation of lead responsibility

ROBO-KNOT Joint Controllership Agreement regulates actions to be taken in the case of the data breaches. In such cases, the Controller where the breach occurs leads the response. If a breach affects joint systems/shared control, Joint Controller 1 (EITDH), PC, coordinates. The mandatory notification to other Controllers is within 48 hours, and it includes to provide a:

- Description
- Consequences
- Mitigation measures
- Requested assistance.

Each Joint Controller may use processors listed in Annex 2. Any proposed change to the processor list requires 30 days prior notice. Controllers must ensure processors meet GDPR requirements including:

- Processing only under documented instructions
- Confidentiality commitments
- EEA-based processing
- Security per Art. 32
- Proper deletion/return of data after service
- Audit and compliance cooperation

Annex 2 lists only one processor for Joint Controller 3 (ADRA)a robotics expert, Talent Selection Committee member.

All GDPR-related notifications must be sent via email to the Contacts listed in Annex 3, that provides primary contact names and email addresses for all 12 Joint Controllers.

Liability is defined according to Art. 82 GDPR. Each Joint Controller is responsible for processing under its factual control. A Controller that breaches GDPR must indemnify others for damages or sanctions exclusively attributable to its actions.

Final Provisions include that Annexes of the Agreement are integral and binding. Invalid provisions do not affect overall validity; they must be replaced with equivalents. Amendments to the Agreement require unanimous written consent; amendments to annexes do not, except changes to Annex 2 (processor list), which require a notification/opposition period. Dispute resolution includes that parties must attempt amicable settlement first; jurisdiction rests with the courts of the defendant’s country.

The ROBO-KNOT Joint Controllership Agreement has three Annexes

- **Annex 1: Description of Personal Data Processing Activities**
  Annex 1 is the most detailed section, covering all personal-data processing activities in ROBO-KNOT. It includes purposes, legal basis, types of data, means, responsibilities, recipients, and retention periods.
- **Annex 2: List of entrusted processors and sub-processors**
- **Annex 3: Joint Controllers' Contact Information**
  Annex 3 lists all contact persons with their name and email address to each of the 12 Joint Controllers.

The agreement establishes a highly detailed GDPR joint-controllership framework, covering:

- Extensive cooperation duties
- Strict GDPR compliance obligations
- Defined roles for all 12 partners
- Comprehensive documentation of all data flows
- Detailed governance of processors
- Clear breach-handling and rights-request procedures
- Structured governance for secondment management and training workflows

It is a mature, multi-party GDPR governance framework designed to support a complex EU-funded mobility project while ensuring transparency, accountability, and fairness.

5. Risk assessment

The ROBO-KNOT project implements a structured and proactive risk assessment procedure to identify, evaluate, and mitigate risks related to data management, GDPR compliance, and multi-partner coordination. The process focuses on anticipating issues that may affect secure data handling, cross-border collaboration, and adherence to legal and ethical requirements.

Mapping specific risk domains is associated with the project's operational and data-processing activities. Each risk category is described in terms of its nature and the underlying reason it may create vulnerabilities.

Risk Area	Description	Likelihood	Impact	Risk Level	Mitigation Measures	Frequency
Crossborder-sharing	Data shared across 12 controllers in multiple countries; potential misalignment	Medium	High	**High**	Unified security standards, shared SOPs	Every 6-months.
Large volume of personal + employment data	Applications contain sensitive career data	Medium	High	**High**	Data minimization, encryption	Every 6-months.
Inconsistent consent management	Not clear how consent is tracked/withdrawn	Medium	Medium	**Medium**	Central consent registry	Every 6-months.
Processor oversight gaps	Missing processors (e.g., Microsoft services)	High	Medium	**High**	Update Annex 2, conduct audits	Every 6-months.
Data breach coordination complexity	Mult controller-controller environment; risk of delays	Medium	High	**High**	Breach response playbook; drills	Every 6-months.
Lack of automated accuracy checks	Risk of outdated information	Medium	Low	**Medium**	Periodic reviews	Every 6-months.

The risk assessment is embedded into the project's broader governance framework (PC, QM, WPLs, PEC and GEA), and is the responsibility of the QM.

6. Ethics

Ethical data handling within the ROBO-KNOT project is grounded in the protection of fundamental rights, particularly privacy, autonomy, and human dignity. Personal data is therefore be processed lawfully, transparently, and only to the extent necessary for clearly defined research purposes. Robust anonymisation or pseudonymisation techniques are applied wherever feasible to minimise re-identification risks, while organisational and technical safeguards ensure confidentiality, integrity, and secure storage throughout the data lifecycle. These measures reduce potential harm to participants and mitigate legal, reputational, and ethical risks associated with misuse or unauthorised disclosure of personal information.

6.1. FAIR Data Principles

As described above, data volumes are expected to remain moderate and document-based, without large experimental datasets, however, due to the presence of the personal data, and the need for publishing project results, ROBO-KNOT consortium utilises FAIR principles.

ROBO-KNOT ensures alignment with the FAIR data principles—Findable, Accessible, Interoperable, and Reusable—through structured data management practices embedded across the project lifecycle. Project outputs, metadata, and relevant research materials are organised within secure, access-controlled repositories using clear naming conventions, version control, and descriptive documentation to support discoverability and long-term traceability. Access conditions are defined according to data sensitivity, intellectual property, and ethical requirements, enabling appropriate sharing while safeguarding confidential or personal information. Standardised formats and commonly accepted vocabularies are used where feasible to support interoperability across institutions and sectors. Finally, clear licensing terms, retention rules, and documentation of provenance facilitate responsible reuse of non-sensitive project results, ensuring that ROBO-KNOT contributes to transparent, high-quality, and sustainable knowledge exchange in line with HORIZON Coordination and Support Action expectations.

6.2. GDPR

The data collector commits to protecting your personal data and respecting your Privacy by collecting and further processing personal data pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

6.3. Gender balance monitoring

In order to capacitate gender balance, ROBO-KNOT project established two separate indicators KPI 1.2 for researchers (and PhDs), and KPI 3.2 for R&I support staff. These two KPIs ensure, that in both target groups the number of female participants will reach at least 30%.

Where relevant and appropriate to the project's objectives, data may be disaggregated by gender to support inclusive monitoring, evidence-based evaluation, and the identification of potential structural inequalities in participation, mobility, skills development, or career progression. Any processing of gender-related or other personal data is conducted in full compliance with GDPR principles, including data minimisation, purpose limitation, and secure handling, while respecting privacy and confidentiality. The project also ensures that gender-sensitive information is interpreted responsibly and used solely to promote equality, inclusiveness, and fair access to opportunities across the consortium.

6.4. Individuals' rights

Individuals have specific rights as a 'data subject' under Chapter III (Articles 13-23) of GDPR, in particular the right to access their personal data and to rectify them in case

their personal data are inaccurate or incomplete. Where applicable, individuals have the right to erase their personal data, to restrict the processing of their personal data, to object to the processing, and the right to data portability.

For the cases where individuals have consented to provide their personal data to the data controller for processing operations, individuals can withdraw their consent at any time by sending an email to roboknot_privacy@28digital.eu. The withdrawal of their consent will not affect the lawfulness of the processing carried out before they have withdrawn the consent.

Individuals can exercise their rights by contacting the data controller, or in case of conflict the Data Protection Officer. Their contact information is given below.

6.5. Contact information

6.5.1 The Data Controller

Anyone in need to exercise their rights under GDPR, or if there are comments, questions or concerns, or anyone would like to submit a complaint regarding the collection and use of personal data, please feel free to contact the Data Controller: roboknot_privacy@28digital.eu.

6.5.2. The Data Protection Officer (DPO)

Individuals may contact the Data Protection Officer (roboknot_privacy@28digital.eu) with regard to issues related to the processing of their personal data under GDPR, and each ROBO-KNOT partner assigned a Joint Controller (name, email) in Annex 3 of the ROBO-KNOT Joint Controllership Agreement.

6.5.3. The Data Protection Authorities

Individuals have the right to have recourse (i.e. they can lodge a complaint) to the competent national data protection authorities (DPAs) according to Art. 56 GDPR (for Hungary this is the National Authority for Data Protection and Freedom of Information (NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság) via the following address: https://www.naih.hu, if they consider that their rights under GDPR have been infringed as a result of the processing of their personal data by the Data Controller.

7. Revisions of the ROBO-KNOT Data Management Plan D4.3

The Data Management Plan (D4.3) is a living document that is periodically reviewed and updated throughout the project lifecycle to reflect evolving activities, data types, ethical considerations, and regulatory requirements, ensuring that any changes in data collection, processing, storage, sharing, or security practices are accurately documented and communicated within the consortium. Updates may be initiated by

PC, QM, WPLs, PEC, GEA, project partners but also by deliverables, technological developments, feedback from quality monitoring, or ethical and legal obligations. If no updates are initiated the QM will review the ROBO-KNOT Data Management Plan D4.3 every 12 months (in M12 and M24).

Each revised version is version-controlled, approved through the project's governance structure, and stored in the shared repository to guarantee transparency, traceability, and continued compliance with FAIR principles, GDPR, and institutional data-management policies.