INNO-NEXT | The Next Generation Innovation Talents' Initiative

European Innovation Council

www.innonext-project.eu
info@innonext-project.eu

Data Management Plan

Deliverable D5.1

Due date of the deliverable: 05/03/2025
Actual submission date: 05/03/2025

Document Information

Deliverable	D5.1	Title	Data Management Plan
Work Package	WP5	Title	Integrated Project Management

Dissemination level[1]	PU	Nature [2]	DMP
Copyright	© INNONEXT Consortium		

Responsible partner	ZUC
Responsible author:	Angelo Schiavone, ZUC
Co-authors	Marco Bernardi, ZUC Carmine Cinquegrana, ZUC Jakub Scholtz, ZUC Juan José Márquez Villacís, LKS Mario Testa, LKS Simone Foglia, RES

Deliverable abstract	This document outlines the methodology for data collection, management, and storage within the project, ensuring compliance with legal and ethical standards. It addresses secure handling practices, retention policies, and ethical risks, including bias in AI applications, while prioritizing privacy and fairness.

Version History

Version no.	Date	Modified by	Actions[3]
V0	19/12/2024	Jakub Scholtz [ZUC]	Creation and outline
V1	17/01/2025	Simone Foglia [RES]	Section 3.2
V2	17/01/2025	Juan José Márquez Villacís, Mario Testa [LKS]	Section 2
V3	20/01/2025	Carmine Cinquegrana [ZUC]	Section 2, 3, 4
V4	03/03/2025	Giuseppe Rizzo [LKS]	Review and quality assurance

[1] Dissemination level: **PU** = Public, **PP** = Restricted to other programme participants (including the JU), **RE** = Restricted to a group specified by the consortium, **CO** = Confidential, only for members of the consortium

[2] Nature of the deliverable: **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other, **DMP** = Data Management Plan

[3] Creation, modification, final version for evaluation, revised version following evaluation, final.

This project has received funding from the European Union (call HORIZON-EIC-2023-TALENTS-01-01), under grant agreement n. 101160467.

Table of Content

List of Figures

List of Tables

Acronym List

EIC	European Innovation Council
EIT	European Institute of Innovation & Technology
ERC	European Research Council
EU PP	European Partner Programme
HC	Hosting Company
HE	Horizon Europe
IN	InnoNext
MSCA	Marie Skłodowska-Curie Actions
PO	Project Officer
VT	Visiting Talent

This project has received funding from the European Union (call HORIZON-EIC-2023-TALENTS-01-01), under grant agreement n. 101160467.

Executive summary

This document outlines the **methodology for effective data collection, treatment, management, and storage** implemented within the project, ensuring compliance with legal, ethical, and technical standards. The methodology is designed to ensure that all data managed through the project's software platform is handled responsibly throughout its lifecycle, from initial collection to final deletion, maintaining transparency and accountability.

The document details procedures for securely collecting data, specifying the types of data involved, their purposes, and the methods used for acquisition. Clear policies are established for data treatment and management within the platform, including access controls, encryption measures, and retention practices, which align with privacy regulations and best practices for data governance. In addition to the data handled via the software, the project also involves managing external documents, such as financial and administrative records, which are stored and processed in separate systems under similarly robust governance practices.

Finally, this methodology places a strong emphasis on **ethical considerations**, particularly in addressing risks such as bias, discrimination, and the misuse of data. Specific measures are implemented to mitigate these risks, especially in the context of AI algorithms, ensuring that human oversight remains central to decision-making processes (human-in-the-loop). By integrating an ethical framework with data management practices, the methodology prioritizes privacy, fairness, and the protection of individual rights, adhering to principles such as privacy-by-design and accountability.

1. Introduction

1.1. InnoNext overview

InnoNext is a European Commission initiative funded under the call HORIZON-EIC-2023-TALENTS-01-01 "Next Generation Innovation Talents", aiming to cultivate an entrepreneurial mindset by creating collaboration opportunities for talented researchers and innovators to work with startups operating in their areas of expertise, across the EU with the support of the extensive network of EIC and various European Partner Programmes.

InnoNext scheme includes 2 open calls dedicated to aspiring Visiting Talents and Hosting Companies to collaborate through an Innovation internship. The calls for interests, which will remain open for the whole duration of the project until 2026, facilitate a tailored matching process. Furthermore, InnoNext offers different resources to connect beneficiaries and support them during the internship, including a comprehensive mentoring and acceleration plan. InnoNext aims to activate 600 internships involving multiple beneficiaries (Table 1).

Table 1 - InnoNext beneficiaries

Visiting Talents	Hosting Companies
Including **PhD candidates, and postdoctoral researchers** participating in projects funded by the following EU Partner Programmes: • EIC Pathfinder • ERC • MSCA Postdoctoral Fellowships • MSCA Doctoral Networks • MSCA COFUND • Research Infrastructures • EIT Label Masters and Doctoral programmes, Alumni, EIT KIC Postdoctoral training programmes	Including startups and **startups and SMEs** supported by the following EU Partner Programmes: – EIC Accelerator – EIC awarded Seal of Excellence – EIC Transition – EIT KIC Innovation and business creation services – Scaleups with at least one EIT Alumni member co-founder.

The InnoNext scheme is structured in six sequential phases (Figure 1) and the following distinctive pillars:

- The **collaboration with the EU Partner Programmes**, which has been involved since the beginning in the call design and during the process through the integrated communication and dissemination of the calls to the potential beneficiaries, as well as the eligibility and monitoring criteria.
- Two **application calls** dedicated to Visiting Talents and Hosting Companies. The calls, largely disseminated thanks to Research and Innovation European Programmes support, will remain open for 18 months. During this period, the continuous monitoring of the process and feedback of beneficiaries and stakeholders might result in the call updates, handled in 5 releases.
- A **dedicated platform** that facilitates the Hosting Companies in creating internship positions and allows Visiting Researchers to apply for them throughout a well-driven and easy process,

supported by dedicated guides and indications. The service includes mechanisms to keep the registered users informed about all the opportunities and suggestions resulting from the matchmaking, the internship activation steps and the mentoring activities, making the whole process understandable and transparent.

- A **hybrid matchmaking process** based on an AI-based algorithm processing the needs and ambitions of the applicants will propose ranked shortlists of opportunities. Shaped and supervised by experts, the whole process will guarantee equal access[4] to opportunities for the applicants.
- **A comprehensive mentorship plan** to offer and share knowledge and tailored support to nurture the entrepreneurship potential of participants. Background and skills such as innovation management, teamwork, and internal communication will be deepened in experiential workshops for Talent and Enterprises. These activities will be planned based on direct feedback collected from the beneficiaries, allowing to improve and refine the InnoNext initiative schema continuously.

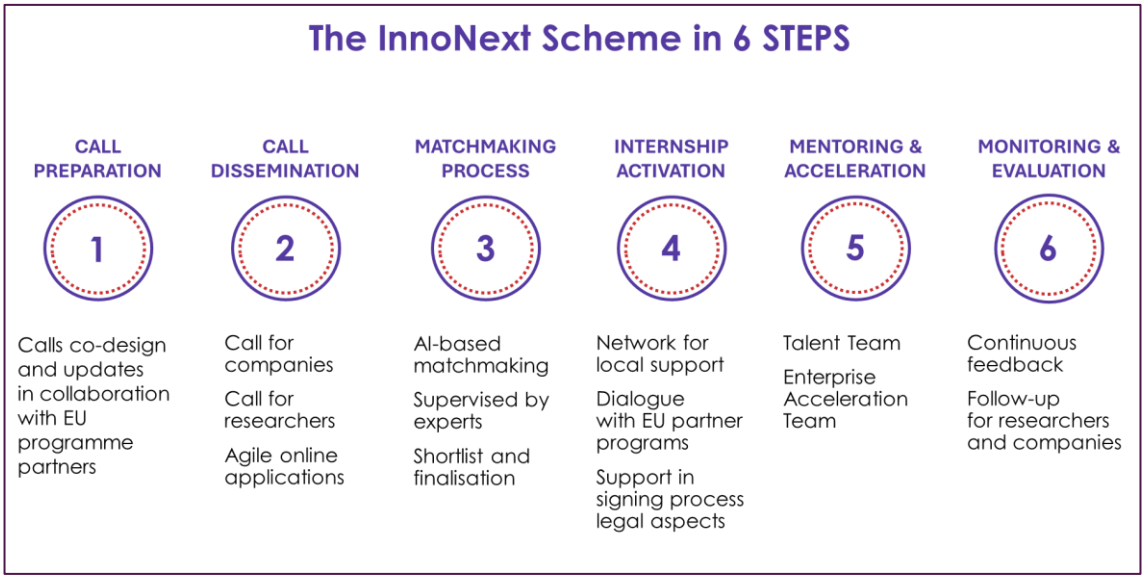

Figure 1 – The InnoNext schema

1.2. Purpose of the Document

The purpose of this document is to present **Deliverable D5.1: Data Management Plan (DMP)**, which outlines the strategies and methodologies for the collection, management, treatment, and storage of data within the InnoNext project. This deliverable provides a unified framework for how consortium partners will handle their data, ensuring consistency and adherence to established privacy, security, and compliance standards, including the **AI Act** and **GDPR**.

The DMP details the responsibilities of each partner in managing their data ethically and securely, addressing potential risks and ethical concerns. It serves as a critical resource to align the

[4] Criteria of fairness and impartiality will be consistently and transparently applied uniformly to the whole process. Every application will have the same opportunities, resources, and consideration without favouritism, discrimination, or any barriers that could disadvantage individuals or groups.

consortium's data practices, ensuring transparent and compliant data handling throughout the project's lifecycle.

1.3. Structure of the document

The document is structured into different sections to ensure a clear and formal presentation of the project's data management practices and ethical considerations. Each section focuses on specific aspects, as outlined below:

- **Section 2** comprehensively summarizes the data collected and managed throughout the project's lifecycle. It highlights the roles of the key stakeholders involved and includes a table summarizing essential details about the data.
- **Section 3** provides a detailed explanation of the policies governing data access and usage, both within and outside the platform. The section emphasizes security measures tailored to the type and purpose of the data and demonstrates adherence to privacy-by-design principles to protect participant privacy.
- **Section 4** examines the ethical challenges posed by the project, particularly concerning AI usage. It describes the measures implemented to prevent biases and discrimination, ensuring ethical standards are upheld.
- **Section 5** concludes with a summary of the key insights and takeaways, emphasizing the importance of responsible data handling and ethical practices.
- **Section 6** – **Annexes** - provides additional documentation and resources that support the topics and claims discussed throughout the deliverable.

2. Data collection overview

Effective data management is a cornerstone of this project, ensuring that all information is handled transparently and responsibly. To support this goal, the following table (Table 2) provides a detailed summary of the project's data assets. It includes information on the types of data collected, their nature (e.g., private or public), ownership, primary users, and the collection methods employed. This structured overview not only clarifies how data is managed and used but also ensures alignment with compliance requirements and ethical standards. By outlining these details, the table serves as a key reference for maintaining accountability and fostering trust in data governance practices.

What follows is an explanation of the column headers used in the table to clarify their purpose and meaning.

- **Data**: refers to the category of information being collected or managed.
- **Description**: provides a brief explanation or summary of what the data represents, its characteristics, or its purpose within the project.
- **Data processor**: identifies the Consortium members responsible for processing the data, who have access to or utilize the data. The purposes for that are explained throughout the document.
- **Type**: indicates the nature of the data, i.e. *Public* (accessible by everyone) or *Private* (managed exclusively by the InnoNext experts, usually involving sensitive data).
- **Collection reasons**: explains the purpose for collecting the data, such as operational needs or user functionality.
- **Collection mode**: describes the method used to collect the data, whether through manual input, automated processes or surveys.

Data processors and users are found among the three members of the consortium, namely:

- **ZUC**, Zucchetti, provider of the *Inrecruiting* ATS, which is adopted as the InnoNext core platform to streamline the publication of available internships, the collection of the talents' applications, and the management of the selection process between HCs and VTs. Inrecruiting also integrates *Inda*, a suite of AI functionalities (including the Job Matching used in the matchmaking process) provided by the same team, which is described in *"D2.1 AI algorithms and the ICT platform"*.
- **RES**, Réseau Entreprendre has expertise in supporting new entrepreneurs and oversees each internship's stage, from supporting Hosting Companies in the talent selection process to the final evaluation step.
- **LKS**, LINKS, the project coordinator and developer of the Competency-based matching, an AI algorithm whose results are combined with the Inda Job Matching's scores to find the top-N talents who are more suitable for each innovation internship.

Finally, RES is the only data controller.

Table 2 - InnoNext data.

Data	Description	Data processor	Type	Collection reasons	Collection mode
Hosting Company profile	Data about the Hosting Companies, e.g. affiliation program and contact information	ZUC, RES, LKS	Private	Allows Hosting Companies to start the registration process for the project	Supplied by each Hosting Company within the platform
Letter of Commitment (LoC)	It is the acceptance of the HC's responsibilities in joining the InnoNext project	RES, LKS	Private	Hosting Company-side eligibility process	Supplied by each Hosting Company via e-mail
Internships	Internship adverts of the positions hosted by the Hosting Companies.	ZUC, RES, LKS	Public	Internship data are published to advertise Hosting Companies' vacancies	Provided by the Hosting Companies within the platform
Talent's CV and data	Talent's CV or resume along with structured data manually inputted	ZUC, RES, LKS	Private	Internship's selection process and matchmaking phase	Supplied by candidate within the platform
Declaration of Honor (DoH)	A declaration that the talent's employer or project coordinator is informed about them joining InnoNext initiative.	ZUC, RES, LKS	Private	Talent-side eligibility process	Talent uploads a DoH on Inrecruiting for each application made on the platform
ORCID	A unique and persistent identifier (PID) for researchers.	ZUC, LKS	Private	Matchmaking process	Supplied by candidate in sign up form
Talent's research outputs	Publications' title, and DOI from CORDIS.	LKS	Private	Matchmaking process	Autonomously retrieved from CORDIS project publications
Additional talent's research outputs metadata (i.e. abstracts)	Publications' abstract, and authors with ORCID.	LKS	Private	Matchmaking process	Autonomously retrieved from open source CrossRef API
Administrative documentation	Internship Agreement between the two parties (HC+VT)	RES, LKS	Private	Internship Activation	The Hosting Company and the Visiting Talent sign the Internship agreement. The Company will share the final version, signed by both parties to InnoNext Team via e-mail.

Financial documentation	Financial Support for Third Parties eligibility check, Financial Agreement, payment's information (FSTP)	RES	Private	FSTP process	Supplied by candidate via e-mail
Communication and Marketing Data	Data generated through InnoNext channels, Website and Social Networks (LinkedIn, X)	RES	Private	Communication and Marketing activities	Cookies tracking, Social Network internal analytics
Feedback and Survey Data	Feedback and insights collected from beneficiaries regarding their experience with the InnoNext Project	RES, LKS	Private	Iterative Scheme Implementation	Survey through Google Forms (regional servers)

3. Data management policies

Key data regarding **talents** and **vacancies** are collected on Inrecruiting, the InnoNext core platform aimed at handling the talent selection process for the Hosting Companies; other data (not handled through the platform) regards administrative documentation and research materials coming from CORDIS, a publicly available database containing EU-funded project publications.

Talent's data include:

- **Personal data**: sourced directly from the candidate via Inrecruiting (described in *"D2.1 AI algorithms and the ICT platform"*), it consists of a manually uploaded CV (curriculum vitae) or résumé file and an application form to fill comprehensive of this information: Name, Surname, E-mail, Gender, Date of Birth, Residence, Phone number, Photo (optional), Country of Employer / Research Institution, University or Research Organization, Affiliate Program, Project Acronym, Project ID, ORC ID, Internship Desiderata (Geography).
  This data is available to both the Consortium and the Hosting Companies, with the main difference being that the Hosting Companies can access only the data related to those who have an application for their vacancies. This happens in two cases:
  - the talent applies spontaneously to the vacancy, proposing themselves for the innovation internship;
  - once a talent has joined the InnoNext project and has applied for a Hosting Company's vacancy, the guidance team of the InnoNext Consortium may find another suitable and available innovation internship for them, thus suggesting the talent to apply.

  This kind of data is later used during the selection process, which is handled by the Hosting Companies and supervised by the dedicated team of the Consortium.

  Talent's data is also shared with Inda (ZUC), the suite of AI algorithms that have been integrated into Inrecruiting, and LKS, since they develop a supporting algorithm for the matchmaking process. Talent's profile can also be exported in a CSV file, useful for producing statistics on the gathered applications and started internships.
- **Publication data**: a collection of talent's papers as found on the CORDIS database (3.1.2).
- **Administrative data**: declarations and contractual documents, such as talent's eligibility declaration in joining InnoNext and beneficiaries' financial records (3.2).
- **Survey data**: evaluation and feedback surveys gathered from visiting talents (3.2).

When a Hosting Company joins the InnoNext initiative in order to become part of the project and to have the opportunity to create internships, it is required to provide the following information: Company name, Company representative, Company size, Company Website, Affiliate program, Project acronym, Project ID, PIC number, Contact First Name, Contact Surname, Contact E-Mail, Contact Telephone number, optional Notes.

To initiate an internship, the Hosting Company first creates a position on Inrecruiting, which becomes publicly accessible on the InnoNext website.

Because of its nature, position data is typically not sensitive and is comprehensive of the fields listed as follows: Hosting Company that opened the position, Title, Company Description, Position Description, Requirements, Additional information about the position, Tags, Workplace, Functional Area, Industry or Sector, Workplace type, and optionally further data like Video URL, Images, Attachments and others.

In addition, each Hosting Company has to send via e-mail (companies@innonext-project.eu) the Letter of Commitment (LoC), which is necessary for the eligibility process and useful for providing information about the Hosting Company (3.2).

Survey data from Hosting Companies are finally collected and stored (3.2).

3.1. Data management on the InnoNext ICT platform

3.1.1. Data privacy and retention policies

InnoNext is committed to full compliance with EU data protection regulations, including the ePrivacy Directive (2002/58/EC) and the General Data Protection Regulation (GDPR, EU 2016/679). Any changes to legislation are closely monitored to ensure that the project's data management practices remain aligned with the latest legal requirements and standards.

Privacy is treated as a core priority, with strict adherence to GDPR principles. Personal data is only shared when necessary and always in full compliance with data protection laws. Robust measures are in place to ensure that privacy is protected throughout the entire data lifecycle.

InnoNext tech platform mainly relies on Inrecruiting and Inda, two products developed by Zucchetti - an Italian multinational company specializing in software solutions and IT services – and hosted on AWS Cloud infrastructure within European regions. This infrastructure ensures compliance with data protection requirements and high standards of security.

Inrecruiting is delivered as a Software-as-a-Service (SaaS) platform and accessed through a web browser. All communications between users and the platform are secured via HTTPS with SSL encryption, ensuring the integrity and security of the data exchanged. A similar approach is used for transferring data to and from the Inda AI solution, which relies on RESTful APIs for its operation. Data is exchanged in JSON format, ensuring consistency and seamless integration between the two systems.

Both Inrecruiting and Inda maintain separate databases for storing talent and vacancy data. To safeguard this information, backups are created regularly, and all data is encrypted using AES-256 both in transit and when archived.

Inrecruiting also adheres to ISO/IEC 27001 standards for information security, ensuring that globally recognized protocols are followed to secure sensitive data.

Access control forms a critical part of the data security strategy. Inrecruiting implements a secure login mechanism to access the platform, requiring users to authenticate before gaining entry. Each session is limited to a 1-hour validity period, reinforcing the system's commitment to preventing unauthorized access by automatically logging out inactive users.

A strict data erasure policy is in place, following the principles of the "Right to Be Forgotten." Talents can request the deletion of their personal data through the InnoNext platform. Upon receiving such a request, the data is immediately and permanently deleted from primary databases and removed from backups within 30 days. Additionally, an automatic deletion policy ensures that all data is retained for a maximum of 2 years after the last update to the candidate's profile but no longer than the project duration. A scheduled cleanup process guarantees compliance with the retention policies and legal obligations. Similarly, Hosting Companies data on the InnoNext platform are retained for the entire project duration, but they can request the deletion of their data at any time.

The data controller is responsible for ensuring the retention policies above, thus verifying the successful deletion of all the data collected and used for the project. Also, in compliance with applicable regulations, talents' data for whom RES is responsible for internship payments, will be retained for 10 years.
In line with industry best practices and standard logging paradigms, InnoNext maintains comprehensive logs to ensure traceability, security, and compliance with relevant standards. Logs are generated to track errors and provide detailed records of actions performed within the platform, ensuring transparency and accountability. The use of logging allows the project to maintain oversight of all system operations, identify potential issues, and ensure the quality and integrity of the data.

3.1.2. Data sharing policies and portability

InnoNext has defined policies for data sharing that prioritize privacy while facilitating collaboration among stakeholders. Internal tech tools, such as Inrecruiting and Inda, have full access to data within the usage policies of the involved entities. However, external entities, such as the talents, are only granted access to their own data and the internship adverts (also known as vacancies). In the case of companies, instead, they have access and can view data related to all the candidates that have applied to one or more of their internship adverts, as well as the adverts they published.
Open access is limited to application forms, which may be shared publicly but only when they are placed on InnoNext website. These policies ensure that data sharing is done responsibly and in compliance with relevant privacy laws.
InnoNext allows candidates to request their personal data to be exported from the system in a portable format, chosen to be CSV. This is facilitated through the Inrecruiting interface, where candidates can download their profile data in CSV format. This mechanism ensures that candidates have control over their personal data and can easily access it in a format that suits their needs.
Also, InnoNext experts export this data for mainly two reasons:

- statistical purposes, enabling the analysis of trends and performance related to recruitment and selection processes. For instance, it is possible to conduct analyses on the demographic characteristics of registered talents to identify potential disparities or areas for improvement in fostering diversity and inclusion. Additionally, statistics can focus on metrics such as the conversion rate of candidates from application to hiring. These insights can help InnoNext monitor and optimize engagement strategies, improve operational efficiency, and ensure fairness throughout the project lifecycle;
- adoption of AI algorithms within the matchmaking process: as discussed in *"D2.1 AI algorithms and the ICT platform",* the Competency-based matching uses talent's ORCID to associate their papers' abstracts and research material found in the CORDIS database.

3.2. Data management for administration and surveys

RES oversees the management of personal and administrative data related to the beneficiaries, not collected in the InnoNext Project Platform. For this reason, it is necessary to provide a brief introduction regarding the operational guidelines for data management and security at RES.
RES is part of a European network, Réseau Entreprendre France, which adopts a rigorous and proactive strategy for data protection. RES aligns with these guidelines, focusing on awareness, training on cybersecurity risks, ethical data management, and risk prevention. Réseau French Federation promotes inside the network initiatives aimed at:

- Raising awareness of the importance of online security through campaigns that highlight best practices and safe online behaviour.
- Providing continuous training to enhance understanding of cybersecurity risks and foster ethical behaviour in data management.

Specifically, the cybersecurity activities are based on four key principles:

1. Multi-Factor Authentication (MFA): Mandatory for all access.
2. Implementation of the "Zero Trust" Principle: Remaining vigilant, not underestimating malfunctions or anomalies, and strictly adhering to security guidelines. In the event of a malfunction, it is mandatory to immediately notify the dedicated cybersecurity team of Réseau French Federation, enabling timely action and risk assessment.
3. Continuous System Updates: Ensuring all devices and applications are kept up to date.
4. Data Protection: Implementing specific measures to safeguard sensitive information.

Data management activities are handled through **Microsoft 365**, specifically utilizing the OneDrive application, provided by the French Federation. Each employee and in-house collaborator within the network have a personal account that grants access to the shared drive.

The Access is secured through strong passwords and multi-factor authentication. Frequent session timeouts are enforced (after 4 hours of inactivity), requiring users to renew their authentication, significantly enhancing overall security. This strategy ensures responsible and secure data management, aligned with the highest cybersecurity standards.
In addition to the infrastructure provided by the French Federation, RES relies on a Data Protection Officer (DPO) who oversees and supports the team in implementing practices aimed at ensuring compliance with current regulations on data management and cybersecurity. In collaboration with

the DPO and in agreement with its partners, RES has developed a Privacy Policy (see 6.1 and 6.2) that governs activities involving interactions with the data of website and platform beneficiaries. Data and information not collected through the InnoNext platform and managed by the RES team mainly because of administrative and monitoring purposes - includes:

1. **Contact Information:** RES manages the official mails of the InnoNext Initiative (info/companies/talents@innonext-project.eu) which allow the team to have the complete access to the Contact Information of the Beneficiaries. In this section are not considered the information collected through the Platform (Company specific information, CV of the Talents etc..), which are managed through the InnoNext Platform Database.
   RES directly manage and use the following data:
   - For Visiting Talents (VT): Name, Surname, E-mail, Phone Number, and information about their affiliation with a specific EU program.
   - For Hosting Companies (HC): Name of the HC, contact details of a representative (Name, Surname, Phone Number, E-mail), Company General Information.

   These data are retained to ensure smooth and immediate communication with the project beneficiaries. A security backup is periodically updated and stored in RES OneDrive. The data will be preserved for the project duration, with the data controller responsible for its deletion at the end of the project. Only those talents' data (including financial documents and agreements) for whom the internship is financed by RES, will be retained for 10 years.

2. **Administrative Documentation:** The administrative documentation encompasses several key categories to ensure compliance, transparency, and proper validation for the project:

   Documents Related to Registration and Eligibility Validation
   - **Declaration of Honour (DoH)**: A formal declaration attesting the talents' program affiliation. DoH helps in the eligibility check of the potential beneficiaries of the Financial Support for Third Parties (only ERC or EIT Pathfinder VT).
   - **Letter of Commitment (LoC)**: A document where the company acknowledges its responsibilities in participating in the InnoNext project, particularly in contributing to the growth of talents.
   - **Internship Agreement**: A contractual document detailing the terms of the internship arrangement.

   Documents Related to Financial Support for Third Parties
   - **Financial Agreement**: A formal agreement outlining financial terms and conditions.
   - **Mobility Allowance Self-Declaration for EIT Pathfinders**: Document attesting to the verification of the talent's workplace location for compliance with the 150 km distance criteria.
   - **Collection of Banking Data**: Information gathered for processing payments.

   Documents Related to Payments
   - **Reimbursements for ERC Participants**: Supporting documents and payment receipts for reimbursements.

- **Mobility Allowance for EIT Pathfinders**: Receipts and documentation evidencing the amounts reimbursed as mobility allowances for EIT Pathfinders.

All documents are securely stored in both physical and digital formats:

- **Digital Archives:** Managed using the Microsoft 365 system provided by the Fédération Réseau Entreprendre. This includes a specially structured digital archive dedicated to the InnoNext project, which must be adhered to by all local branches.
- **Physical Archives:** Maintained at the REP headquarters located in Via Maria Vittoria 38, Torino 10123, Italy. The Physical Archives is dedicated to the Agreements, supporting payment documents and Timesheet related to the Internship Activation.

3. **Communication and Marketing Data:** RES is responsible for monitoring, collecting, and managing data generated through communication and marketing activities on the innonext-project.eu website and Social Networks (LinkedIn and Twitter). The management of such information is conducted using Social Network internal analytics and tracking cookies obtained through:
   - Google Analytics for the website;
   - Meta Pixel;
   - LinkedIn Insight Tag.

   The data collected includes page views, which do not contain information about user behaviour or conversion factors.

4. **Feedback and Survey Data**: During the project implementation phase, evaluation and feedback surveys will be distributed to participants to gather feedback and insights regarding their experience with InnoNext Project, under RES' oversight and responsibility. The surveys are designed using Google Forms and include sections for collecting personal information such as First Name, Last Name, Gender, Level of Education, Origin, and Affiliation Program. Additionally, information about participants' experiences prior to and during their involvement in InnoNext will also be gathered. Data will be collected for both VT and HC and used to improve and tailor the service to the emerging needs of the beneficiaries. The collected data will be stored in the archives for the duration of the project, in compliance with data protection regulations. For data collection through Google Forms, RES establishes the use of **regional servers** in compliance with EU regulations. Geographic localization enables better threat management, as security measures are tailored to the specific regulatory and environmental requirements of the region. This system protects sensitive data, strengthens user trust, and ensures legal compliance. After the project's conclusion, the collected information will be preserved with the aim to product monitoring and evaluation reports. The reports will provide a comprehensive overview of the initiative, allowing for an analysis of the project's impact, identification of best practices, and development of future strategies.

4. Ethical risks

The collected data serves several functions within the InnoNext project; it is managed according to the discussed reference, description, scope, and goal, with the aim of enabling accurate and efficient talent-internship matching.

To ease this task, InnoNext employs AI algorithms to compare a list of talents (or a list of internships) with a specific internship (or talent), producing a relevance score that reflects the degree of compatibility between the two. This score is then used to rank talents (or internships) in descending order, providing recruiters with a structured and prioritized list to support their decision-making process. While this approach introduces efficiencies and adds value by simplifying the evaluation of multiple options, the system adheres to a "human-in-the-loop" principle, ensuring that all final decisions are made by human recruiters. By ensuring that human oversight is incorporated at key stages, this principle mitigates risks associated with algorithmic bias, errors, or unintended consequences. It allows for nuanced judgment, ethical considerations, and contextual understanding that machines cannot replicate. It also fosters accountability and trust by keeping humans responsible for final decisions, ensuring that technology complements rather than replaces human expertise. The AI serves purely as a decision-support tool, offering recommendations without excluding candidates or making independent determinations. Such tools help InnoNext experts support Hosting Companies in making their decisions.

Despite its potential benefits, the use of AI in this context introduces several ethical risks. One key concern is the possibility of algorithmic bias, where patterns or prejudices present in the training data might influence the relevance scores. For example, if the historical hiring data used to train the algorithm reflects societal biases—such as a preference for certain demographics, educational institutions, or career paths—these biases could inadvertently be reinforced. This can lead to systematically disadvantaging certain groups, resulting in discriminatory practices even if unintended. Additionally, there is the risk of automation bias, where recruiters may over-rely on the system, perceiving the AI-generated recommendations as fully objective or infallible. This can undermine critical human judgment and lead to decisions that are not fully aligned with the goals of fairness and inclusivity.

To address these risks, a multifaceted approach has been adopted. First, the AI system itself undergoes rigorous audits and testing to identify and mitigate any biases in its training data or algorithms. This includes ensuring that the data used for training reflects a diverse and representative sample, as well as actively working to detect and neutralize patterns of historical discrimination. Second, the system is designed to prioritize transparency. This involves providing recruiters with explanations of how relevance scores are calculated, what factors are considered, and the inherent limitations of the algorithm. Such transparency ensures that users understand the system's role as an aid to their decision-making and remain critical evaluators of its outputs.

Feedback mechanisms are also established, enabling stakeholders to report any concerns or anomalies related to the algorithm or event participation processes. This feedback can then be used to continuously refine and improve the system and organizational practices.

Finally, privacy and data protection are paramount. The system adheres to strict data retention and security policies, ensuring compliance with legal regulations and ethical guidelines. All personal data are handled transparently, with participants informed of how their data is being used, for what purposes, and for how long it will be retained (Annexes 6.1 and 6.2).

By addressing both the algorithmic and procedural dimensions of ethical risks, the system can support fair, transparent, and inclusive practices. Combining robust technical safeguards with thoughtful organizational measures ensures that the AI system not only enhances efficiency but also aligns with broader goals of equity and ethical responsibility, creating a positive impact on both the decision-making process and stakeholder engagement.

In conclusion, the system adheres to the requirements of the AI Act by integrating key compliance measures at every stage of its development and operation. For instance, the system incorporates mechanisms for transparency, such as clearly informing users when AI-driven algorithms are employed in the matchmaking process. It also follows strict guidelines for data protection by implementing privacy-by-design principles and ensuring secure handling of personal information in alignment with GDPR. Furthermore, the system addresses potential ethical risks by integrating the human-in-the-loop principle, ensuring that final decisions always involve human oversight to prevent bias or discrimination. These features demonstrate the system's commitment to meeting the AI Act's standards for ethical, secure, and transparent AI applications.

5. Conclusion

InnoNext has implemented a comprehensive and structured methodology for data management, ensuring the highest standards of security, privacy, and ethical responsibility. Throughout its lifecycle, from data collection to final deletion, each stage has been carefully designed to safeguard both the integrity of the data and the privacy of individuals involved.

Key to this methodology is the secure handling of data within the project's platform, with defined protocols for access control, encryption, and retention. Additionally, the management of external documents, such as financial and administrative records and surveys, follows strict governance practices to maintain consistency across all data sources.

Equally important is the emphasis placed on data storage and security, with compliant infrastructure, regular backups, and secure deletion protocols in place to ensure data is protected and handled in line with regulatory requirements.

Finally, the ethical framework integrated within the methodology remains a fundamental pillar of the project, addressing potential risks such as biases or misuse of AI. The project has put measures in place to mitigate these risks, ensuring that human oversight continues to be at the core of decision-making processes. By embedding privacy-by-design principles, fairness, and accountability, the methodology ensures a responsible and transparent approach to data governance, while prioritizing the rights and protection of all involved stakeholders.

6. ANNEXES

6.1. *Visiting Talents Privacy Policy*

Available both on InnoNext website and platform, the Visiting Talent Privacy Policy ensures that internship applicants gain a clear understanding of how their personal data is collected, used, and protected throughout the selection process. This policy outlines the types of data processed, the purposes for its use, and the measures taken to ensure compliance with data protection regulations such as GDPR. It emphasizes transparency, security, and the rights of individuals to control their information, fostering trust and accountability in data handling practices.

6.2. *Hosting Companies Privacy Policy*

The Privacy Policy for Hosting Companies participating in the project outlines how their data is collected, used, and protected in compliance with relevant regulations, including GDPR. It details the types of information processed, such as company profiles and contact details, the purposes for data use, and the security measures in place to ensure confidentiality. This policy ensures transparency, safeguards sensitive information, and establishes a foundation of trust between the project and the participating companies.

INNO--NEXT | The Next Generation Innovation Talents' Initiative

European Innovation Council

InnoNext is an initiative funded by the European Union
(call HORIZON-EIC-2023-TALENTS-01-01) under grant agreement n. 101160467.

www.innonext-project.eu | *info@innonext-project.eu*

InnoNext Consortium:

FONDAZIONE links PASSION FOR INNOVATION

Réseau Entreprendre

ZUCCHETTI