

INVEST Digital Services

Privacy Notice

Publication draft 1.0 | Prepared 26 October 2026

Effective for each service upon approved publication

1 Scope and service access

This notice explains how personal data are handled through the INVEST digital services listed below. It covers public browsing, accounts, educational and mobility administration, educational and research resources, academic and career guidance, research collaboration, and related support. Read the common sections together with the section for the service you use.

Service	Entry point
Virtual Campus	https://virtualcampus.invest-alliance.eu/
Microcredential and Lifelong Learning Platform	https://microcredentials.invest-alliance.eu/
Mobility Journal	https://mobilities.invest-alliance.eu/
Open Science Hub	https://virtualcampus.invest-alliance.eu/Site/Home/OnlineRepo
Open Repository	https://dspace.invest-alliance.eu/
EDUC8EU	https://educ8eu.invest-alliance.eu/
Research Excellence Centre Platform	https://centreofexcellence.invest-alliance.eu/

The Internship and Job Finder and the Quality Assurance Modeler are also covered from activation of the respective service or authorised pilot that links to this notice.

Institutional student records, learning environments, funding agreements and third party websites may have additional privacy information. A separate notice applies to processing that falls outside this scope. Before collecting information for a new purpose, the responsible institution must provide the relevant information.

For service coordination and help directing a privacy request, contact Omiros Iatrellis at iatrellis@uth.gr. You can also contact the relevant institution or data protection officer directly, using the directory in Section 2.

2 Responsible institutions and contact routes

The INVEST partner universities are listed below. Responsibility follows the processing concerned. For the shared Mobility Journal workflow, the seven universities jointly determine the purposes and essential rules and act as joint controllers. The home institution handles outgoing applications and its decisions; the host institution handles incoming review and hosting arrangements. The University of Thessaly provides the shared technical operation and system administration.

For other services, the institution offering the programme, issuing the credential, managing the collection, handling the research request, running the institutional advising activity or supplying quality assurance records is responsible for its own institutional processing. Where partner universities jointly determine a shared processing activity, they act as joint controllers for that activity. Technical administration alone does not determine who is the controller.

For shared processing, the practical contact routes are the common service contact for technical coordination and the relevant institutional contact for substantive decisions and data protection matters. Authorised staff handle records within their assigned institution or workflow. A common platform does not authorise every partner to inspect every personal record. You may exercise your rights against any joint controller involved in the processing.

For processing under joint controllership, an Article 26 GDPR arrangement must allocate the institutions' responsibilities. Its essential terms must be made available to the individuals concerned. Use the contact routes below to request information about the allocation of responsibilities for your processing.

Institution	Address and privacy contact
Slovak University of Agriculture in Nitra Slovakia	Tr. A. Hlinku 2, 949 74 Nitra, Slovakia Data protection officer: zodpovedna.osoba@uniag.sk
University of Agribusiness and Rural Development Bulgaria	78 Dunav Boulevard, 4003 Plovdiv, Bulgaria Institutional contact for routing a data protection request: uard@uard.bg
University of Thessaly Greece	Argonafton and Filellinon, 38221 Volos, Greece Data protection officer: dpo@uth.gr
Karelia University of Applied Sciences Ltd Finland	PO Box 256, 80101 Joensuu, Finland Data protection contact: tietosuoja@karelia.fi
University of Córdoba Spain	Avenida Medina Azahara s/n, 14071 Córdoba, Spain Data protection officer: dpdatos@uco.es
Université de Reims Champagne-Ardenne France	2 avenue Robert Schuman, 51100 Reims, France Data protection officer: dpo@univ-reims.fr
Università degli Studi di Milano-Bicocca Italy	Piazza dell'Ateneo Nuovo 1, 20126 Milano, Italy Data protection officer: rpd@unimib.it

If the responsible institution is unclear, name the service and the relevant programme, record, collection or application in your request. The common contact will help route it. Please avoid sending an identity document or sensitive supporting material in an initial email.

3 Information used by each service

Virtual Campus

Virtual Campus uses account and institutional identity information, such as name, institutional email, affiliation, student or staff identifier where relevant, assigned roles and authentication records. Depending on the functions used, it also handles programme and course participation, applications, academic activity, study outcomes, mobility administration and communications. Authorised institutional officers maintain their institutional records and review requests. Account and technical information supports access, support and security.

Microcredential and Lifelong Learning Platform

The platform handles programme registrations, learner identity and contact information, eligibility, participation, assessment status, award decisions and badge information. The university providing the learning activity is responsible for its assessment and award decisions. Public course descriptions are

separate from private participant records. Credential verification can disclose award and issuer information, and recipient or evidence information included in the credential. The issuer must explain the personal information exposed by its verification or sharing method before issuing the credential.

Mobility Journal

Mobility Journal handles identity and contact details, institutional affiliation, participant category, relevant study or employment information, home and host institutions, activity, destination, dates, relevant language and ECTS information, funding category, review status, correspondence and completion information. Relevant administrative documents can accompany the application where required.

The Mobility Journal applicant process does not request passport or identity document numbers or copies. The fewer opportunities field records a Yes or No response. It does not request a medical diagnosis, disability explanation or medical certificate. An indicator or its context can still reveal sensitive circumstances. Institutions must limit access and use an appropriate separate process, with an applicable Article 9 GDPR condition where required, for sensitive support information.

Open Science Hub

The Hub handles publication metadata and files, including author names, affiliations, scholarly identifiers, titles, abstracts, references, licences and contributor information. Submission and curation records can also include private contact details and review correspondence. Public scholarly records are distinguished from private accounts and administrative notes. Where a publication is deposited through the Hub in Zenodo, the approved metadata and files are sent to Zenodo. Published records can be discovered through OpenAIRE and onward discovery services, including EOSC.

Open Repository

The DSpace repository handles account details, affiliation, contributor and curator roles, deposit metadata, submitted files, permissions, review decisions and correspondence. Published records may identify authors, contributors and institutions and include scholarly identifiers and licence information. An uploader must have authority to submit information about other people. Private account email addresses and review notes are distinct from metadata selected for publication. Collection rules determine whether a file is public, restricted or under embargo.

EDUC8EU

EDUC8EU processes information supplied during study and career exploration, including academic context, RIASEC interests, perceived learning factors, skills, selected pathways, assessment responses, recommendations and conversational inputs and outputs. The information interface can include affiliation, student identifiers, names, country and prior degree information when supplied. The public advising journey can be used without an account. Information entered in an assessment or conversation can identify a person even when no sign in is required. OpenAI processing is explained in Section 6.

Research Excellence Centre Platform

The Centre of Excellence handles research cluster and professional profile information, expertise, affiliations, institutional contact details, collaboration enquiries and facility or infrastructure requests. Request records can include the requester, purpose, proposed activity, correspondence and institutional decision. Professional information designated for publication is separate from private requests. The institution managing a profile, facility or request handles the relevant content and substantive decision.

Internship and Job Finder

When activated, Job Finder processes applicant identity, contact and affiliation information, study and career profiles, CVs, skills, preferences, opportunity information, applications, review outcomes and related correspondence. Applicants, university officers and the organisation receiving an application

have different roles. Sending an application discloses its contents to the selected organisation and the authorised institutional officers involved. An organisation independently handling recruitment must provide its own privacy information. AI assisted skill extraction and matching can use OpenAI as described in Section 6.

Quality Assurance Modeler

When activated, QAM processes organisational structures, indicator assignments, source records, evidence, validation decisions, feedback and improvement actions. Records can concern students and staff where individual information is necessary for an authorised institutional quality assurance activity. The institution supplying the information controls its institutional use; shared Alliance reporting should use aggregated information where identification is unnecessary. Identifiable staff evaluation and student records require restricted access. New processing with a likely high risk requires an assessment before it begins.

4 Sources and information you provide

Information comes from you, the institution used to access a service, authorised institutional staff, contributors and curators, organisations receiving applications, and public scholarly or programme sources. Authentication can supply the identifiers and attributes needed for the requested access. Institutions can import or correct authorised records. Public research records may include information supplied by a coauthor, depositor, publisher or indexing service. The relevant institution can explain the source of information concerning you.

Technical information can include IP address, browser and device information, session identifiers, authentication events, access times, errors and actions needed for operation and security. The technical information collected depends on the service and the feature used. Optional analytics are described separately below.

Required fields must be identified in the relevant process. Without information necessary for an application, award, deposit, account or request, the responsible institution may be unable to provide that function. Optional information can be omitted. Please submit only relevant material and avoid including information about other people or sensitive personal circumstances unless the institution has requested it through an appropriate process.

5 Purposes and legal grounds

Personal data are used to provide the function selected, administer participation, maintain accurate academic or professional records, communicate decisions, manage approved public resources, respond to enquiries and protect the service. The applicable legal ground depends on the activity and the responsible institution.

Article 6(1)(e) GDPR applies to educational administration, mobility, institutional guidance, scholarly dissemination and quality assurance where the relevant task is vested in the institution by applicable EU or national law. The institution must identify the task and legal framework supporting its processing. Technical operation and proportionate security measures necessary for that task follow the same purpose and applicable basis.

Article 6(1)(b) applies where processing is objectively necessary to take steps you request before entering an agreement, or to perform an agreement with you, such as an applicable participation or deposit agreement. Article 6(1)(c) applies to a specific statutory reporting, accounting, employment, audit or other legal obligation. A grant agreement alone does not make every processing activity a statutory obligation.

Article 6(1)(f) can apply to proportionate interests such as service security or management of voluntary professional contacts where that basis is legally available and the required balancing assessment supports it. Public authorities cannot rely on that basis for processing performed in carrying out their public tasks.

Article 6(1)(a) applies where consent is sought for an optional activity, including optional analytics or an optional publication feature that relies on consent. You may refuse or withdraw such consent without affecting processing necessary for the main service. Accepting the Terms of Use, acknowledging this notice or licensing a file does not provide blanket GDPR consent. Processing special category data additionally requires an applicable Article 9 condition.

6 Access recipients and external services

Access is limited to the people who need information for the relevant activity: the user, authorised institutional officers, assessors or curators, relevant home and host staff, credential issuers, and technical administrators performing support or security work. Approved providers may support hosting, authentication, email, recovery, analytics or protection against automated misuse under the applicable arrangements. Where required, necessary information can be disclosed to funding bodies, auditors or competent public authorities.

Public records and application recipients

Published scholarly records, approved professional profiles, resource metadata and files selected for open access are available to the public. They can be indexed, downloaded, cited and reused worldwide under the applicable licence and data protection rules. Restricted files, private applications, assessment responses and administrative notes must not be made public merely because the service has a public catalogue. Job Finder application information is shared with the selected organisation as part of the requested application process.

OpenAI assisted guidance and matching

OpenAI models support EDUC8EU conversational guidance and the planned Job Finder AI functions. The information submitted to an AI feature and the relevant study or career context used to generate its response can be processed by OpenAI. Inputs can contain personal information, including information entered in free text, assessment or CV content used for the requested function. Please keep submissions relevant and avoid unnecessary identifiers and sensitive information.

The institution operating the feature must limit the information sent to what the function requires and explain the applicable processing before using it. Removing a name alone does not necessarily make information anonymous. Provider processing locations and retention depend on the feature configuration and institutional agreement. Those arrangements must be explained for the feature used.

OpenAI publishes information about its data handling at

<https://developers.openai.com/api/docs/guides/your-data> and <https://openai.com/policies/privacy-policy/>. Those documents describe provider services and available configurations; the applicable institutional configuration remains relevant. An INVEST retention period for its own copy does not automatically set the retention of provider copies. Information about the processing affecting your use can be requested through the common contact.

Zenodo and scholarly discovery

The Open Science Hub connects to Zenodo through its deposit interface. CERN operates Zenodo under its own data protection framework and privacy policy. Approved scholarly metadata and files can become public on Zenodo; OpenAIRE can collect published records and make them discoverable through wider research services, including EOSC. This is an indirect discovery route rather than a direct deposit into an EOSC service. Zenodo has its own retention, correction and withdrawal rules: <https://about.zenodo.org/privacy-policy/> and <https://about.zenodo.org/policies/>.

Google services and cookies

Google Analytics is used for activity reporting on Virtual Campus, Microcredentials and Mobility Journal. The policy for optional analytics requires a prior choice through the applicable cookie controls. Refusing or withdrawing optional analytics consent must not prevent use of the essential service.

Identifiable analytics event and user data are subject to a two month retention setting; irreversibly anonymous aggregate reports can be kept longer.

Mobility Journal uses Google reCAPTCHA to protect its application process from automated misuse. It assesses technical interaction signals and can use security cookies. Essential technologies also support sign in, session security and saved cookie choices. Each service must identify its own active technologies and provide the required controls; the presence of a provider in one INVEST service does not imply its use in another. Contact iatrellis@uth.gr if an access challenge prevents use of a service.

7 Hosting and international processing

UTH provides the shared technical operation for Mobility Journal, whose main application data are hosted on a dedicated UTH server in Greece. Its recovery policy requires copies under UTH control within the European Economic Area. For other services, hosting and technical operation follow the arrangements of the responsible institutions and their approved providers. The common contact can identify the operator and relevant processing locations for your service.

External processing by OpenAI, Google or scholarly infrastructure can involve locations outside the EEA or an international organisation. An EEA location for a main application does not establish that every recipient processes information only within the EEA. Public scholarly publication also makes the approved content accessible worldwide.

A transfer requiring Chapter V GDPR safeguards must be supported by an applicable mechanism, such as a relevant adequacy decision or appropriate contractual safeguards, with additional measures where required. Institutions must identify the relevant recipient, destination and safeguards before transferring personal information. You can request information about a transfer concerning you and a copy of the relevant safeguards through the contacts in Section 2.

8 Retention and deletion

The following schedule sets the routine policy for INVEST controlled service records. It distinguishes working platform copies from authoritative institutional records and public scholarly content. A period starts from the event stated in the table. Administrative closure means that the activity, required completion and financial steps, and any pending review or appeal have concluded.

Record category	Routine retention policy
Unsubmitted applications and unfinished deposits	90 days after the last relevant user activity.
Unsuccessful or withdrawn applications and rejected deposits	12 months after the final decision or withdrawal and the end of any review or appeal.
Routine completed mobility and participation records	24 months after administrative closure, unless an applicable institutional, funding or legal schedule requires the record.
Account contact details and assigned access roles	For the authorised account lifetime and 12 months after closure, unless required for an associated retained institutional record. Public authorship and award evidence are assessed separately.
Saved EDUC8EU assessments and conversations	12 months after the last advising activity. Retain a longer research or statistical dataset only under an applicable separate basis and notice, or after irreversible anonymisation.
Job Finder profiles and CVs	For the active profile lifetime and 12 months after account closure. Application copies follow the application rule; a necessary placement record follows the participation rule.

Record category	Routine retention policy
Closed research collaboration and facility requests	24 months after closure. A resulting agreement or official institutional record follows its applicable institutional schedule.
Routine access and security logs	180 days from the event. Preserve only a necessary incident subset for a documented investigation or legal hold.
Routine support correspondence	12 months after closure. Formal complaints and rights request files follow the responsible institution's applicable schedule.
Identifiable optional analytics event and user data	Two months. Irreversibly anonymous aggregate statistics may be retained longer.
Recovery backups	A rolling maximum of 90 days. After deletion from an active system, a remaining recovery copy expires within a further 90 days.

Academic awards and quality assurance records

Authoritative student records, transcripts, issued credentials and the minimum evidence needed to verify an award follow the issuing institution's academic retention or archival requirements. There is no automatic 24 month expiry for a valid credential or its necessary verification record. The issuer can explain the applicable period or retention criteria.

QAM keeps identifiable source and working evidence only for the defined institutional reporting cycle and associated validation, review and appeal needs. The responsible institution must set and communicate that schedule before importing identifiable information. Necessary official QA evidence follows the applicable institutional or accreditation schedule; irreversibly anonymous indicators can be retained longer for comparison.

Published resources and professional information

Published repository and Hub files, bibliographic metadata, scholarly authorship, licences and necessary provenance are retained while needed for lawful dissemination, attribution, verification and preservation. Review is triggered by a correction or withdrawal request, a rights issue, or collection review. This preservation criterion does not justify indefinite retention of unrelated private account or review information.

Public professional profiles and contact details are retained while current and relevant to the listed role and are reviewed when a role ends or a correction is requested. A withdrawn resource may leave a minimal reference or tombstone where justified for citation integrity or legal evidence. Retain only necessary personal fields. Removing a local record does not automatically remove an independent Zenodo record, an index entry or a lawful third party copy.

Legal obligations and recovery copies

A specific legal requirement, signed funding agreement, official institutional schedule or documented audit, dispute or legal hold can require the necessary records for longer. The applicable rule and starting event determine the period. Where a grant requires evidence for five years after final payment, retain the necessary evidence for that period, rather than extending every field and attachment automatically. Restrict and review information retained under a hold.

Before deleting an authoritative record, transfer it to the governed institutional archive where required. Recovery copies are used for recovery rather than routine review. A restore must not restart a retention period; prior deletion instructions must be reapplied before restored records return to ordinary use.

9 Security and decisions affecting you

The services use HTTPS and authorised roles for protected functions. The operating policy requires proportionate access restrictions, confidentiality, secure credentials, updates and recovery arrangements. For centrally operated records, the recovery standard requires daily encrypted backups, restricted technical access and the retention limits in Section 8. Technical support access must be limited to the support or security task. Report suspected unauthorised access privately to iatrellis@uth.gr without retrieving or disclosing another person's information.

Academic, mobility, recruitment, facility access and quality assurance decisions remain subject to the responsible institutions' or organisations' authorised procedures. EDUC8EU recommendations and Job Finder matching assist exploration and review. They do not themselves grant admission, award credit, select an applicant for employment or determine a staff assessment. Technical validation and administrative notifications may be automated.

If a future process uses solely automated decision making with legal or similarly significant effects, the responsible institution must first explain the basis, logic, significance and applicable safeguards. Where Article 22 GDPR applies, safeguards include the opportunity to obtain human intervention, express your view and contest the decision. Introducing such a process requires appropriate prior information and assessment.

10 Your rights and complaints

Depending on the processing and legal basis, you may request access, correction, erasure, restriction and data portability where its conditions are met. You may object on grounds relating to your particular situation where processing relies on a public task or legitimate interests. Where processing relies on consent, you may withdraw it at any time without affecting earlier lawful processing. Some records must be retained under applicable law or another permitted exception.

Send requests to the relevant institution or use iatrellis@uth.gr for routing, or dpo@uth.gr for the UTH data protection officer. Identify the service and, if available, the record reference. A proportionate identity check may be needed; do not send an identity document unless specifically requested through an appropriate route. Any joint controller involved can receive a rights request.

Requests must be handled without undue delay and normally within one month. A GDPR permitted extension for complexity or number of requests must be explained within the first month. Requests are normally free; a reasonable fee or refusal is permitted only under the conditions established by the GDPR.

You may complain to a competent supervisory authority, including the authority where you habitually live or work or where an alleged infringement occurred. For UTH, the competent authority is the Hellenic Data Protection Authority at <https://www.dpa.gr/>. Contacting the service first is helpful but is not a prerequisite for a complaint.

11 Publication and changes

This common notice takes effect for a listed service when the approved version is published and linked from that service. It supersedes an earlier service notice only for the processing it expressly covers. The publication date and version must remain visible. Relevant information must be accessible when personal information is collected, including at application, registration, deposit and AI interaction entry points.

Material changes to purposes, recipients, retention or other processing arrangements must be communicated before the changed processing begins. Publication does not create retrospective consent or change the legal basis for earlier processing. An institution introducing a new collection purpose, sensitive data use or higher risk feature must provide the corresponding information and safeguards before activation.