KreativEU

Knowledge & Creativity
European University

D1.5

Data Protection Plan

Version 1.0 | June 2025

Co-funded by
the European Union

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 Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

D1.5

Data Protection Plan

Project Acronym:	KreativEU
Project full title:	Knowledge and Creativity European University
Project No:	101177256
Funding Scheme:	ERASMUS + Programme under call ERASMUS-EDU-2024-EUR-UNIV
Coordinator:	IPT · Polytechnic University of Tomar
Project start date:	01.01.2025
Project duration:	48 months

Deliverable:	D1.5 – Data Protection Plan
Contractual date:	June, 30th (M6)
Deliverable date:	June, 30th (M6)
Work package:	WP1 – KreativEU Governance and Management
Task:	T1.6 – Cybersecurity and Data Protection policies, procedures and reporting
Dissemination Level:	SEN · Sensitive
Contributors:	This deliverable was produced by the KreativEU Data Protection Team (led by the Polytechnic University of Tomar) with contributions from all partners.
Abstract	This document sets forth the policy and procedures at KreativEU to safeguard individuals' rights and freedoms in relation to person data and in compliance with national and EU legislation.

Table of contents

Data Protection Plan

Executive Summary

This Deliverable, D1.5 – Data Protection Plan –, developed within the Erasmus+ project KreativEU (101177256 – ERASMUS-EDU-2024-EUR-UNIV) under Work Package 1 – KreativEU governance and management, signed by all the HEIs involved, will set the policy and procedures at KreativEU to safeguard individuals' rights and freedoms in relation to personal data and in compliance with national and EU legislation. In line with the General Data Protection Plan (GDPR) and national data protection laws, this Data Protection Plan outlines the principles, responsibilities and procedures for safeguarding personal data processed within the Alliance.

This plan ensures that all member institutions uphold a consistent and high standard of data protection, promoting trust, transparency and accountability in all joint activities – whether in research-based activities, education, administration or digital services.

The Data Protection Plan has been prepared collaboratively by the KreativEU Data Protection Team (led by the Polytechnic University of Tomar), with the assistance of the Project Coordinator and the cooperation of the Data Protection teams of each of the partner institutions, ensuring alignment with the local data protection plans.

1. Governance and Accountability

This section defines the leadership and oversight structure for data protection:

- **Data Protection Officer:** in accordance with KreativEU's Consortium Agreement, the Consortium Leader appoints a Data Protection Officer.
- **Data Protection Team:** A cross-institutional body, described in the Consortium Agreement, that ensures harmonized implementation of GDPR across all partners.
- **Joint Controllership Agreement:** a legal document that clarifies how responsibilities are shared when multiple institutions process or transmit data jointly.
- **Data Protection Policy:** a formal document, to be publicly displayed at KreativEU's website, that outlines how the alliance collects, uses, stores, protects, and shares

personal data in compliance with the General Data Protection Regulation (GDPR) and other relevant data protection laws.

2. Data lifecycle management

This section covers how personal data is handled, from collection to deletion:

- **Collection:** data must be collected lawfully, with clear purposes and consent where required.
- **Storage:** data is stored securely using encryption and access controls.
- **Usage:** data is only used for the purposes for which it was collected (e.g., student mobility).
- **Sharing:** data sharing among institutions is governed by formal agreements and GDPR safeguards.
- **Data in Transit:** all data should be encrypted when transmitted across networks (internal & external) using TLS/SSL or equivalent protocols.
- **Retention and deletion:** data is kept only as long as necessary and securely deleted when no longer needed.

3. Risk management

This section focuses on identifying and mitigating risks, involving the production of templates, to be used by the entities within KreativEU, for:

- **DPIAs (Data Protection Impact Assessments):** required for high-risk processing activities, such as using AI or handling sensitive data.
- **Incident Response Plans:** a coordinated approach to managing data breaches, including notification procedures and mitigation steps.

Risk management is divided in the following steps:

- **Detection and Identification:** Each institution should establish monitoring systems to detect unauthorized access and anomalies in data systems;
- **Reporting:** any data breach must be reported to the institution's DPO within 24 hours;
- **Assessment:** The DPO assesses the scope, nature, and severity of the breach;

- **Notification:** Data subjects are notified without undue delay where applicable. Supervisory Authorities must be notified within 72 hours, in compliance with GDPR Article 33;
- **Documentation:** All incidents must be documented in a breach log shared annually with the Consortium DPO.

4. Compliance and Auditing

In this section, legal and procedural adherence with respect to privacy, artificial intelligence and data processing are concerned:

- **Legal Framework:** GDPR, national laws of each member country and KreativEU's Consortium Agreement.
- **Audits:** According to and with compliance with the Consortium Agreement, assessment of the implementation of the Data Protection Plan is taken every six months during the lifecycle of the consortium, reported to the Steering Committee.
- **Documentation:** Records of Processing Activities (ROPA) are maintained, to demonstrate accountability.

5. Training and Awareness

Promotes a culture of data protection and awareness, via:

- **Expected Training:** all involved in data processing are expected to receive training, in order to be updated in what concerns with data protection issues.
- **Awareness campaigns:** initiatives to educate the community about rights and responsibilities.

6. Technology and Security

Addresses the technical infrastructure:

- **Secure platforms:** use of GDPR-compliant tools for communication, data storage and collaboration.
- **Access controls:** role-based access and multi-factor authentication to protect data.

- **Privacy-by-design:** ensuring that all systems and services are built with data protection in mind from the outset.


KreativEU
Knowledge & Creativity
European University