

Digital Innovation Gateway or Kosovo (DIG-4K)

Digital Europe Programme

This project has received funding from the European Commission's Digital Europe Programme

Project number: 101191620

Start date: 2025-01-01 Duration: 48 Months

<https://itp-prizren.com/dig-4k/>



Data Management Plan

Document Title	Data Management Plan
Author(s)	
Number of pages	
Document type	Deliverable
Work Package	WP1
Document number	D1.2
Issued by	Innovation and Training Park, ITP Prizren
Date of completion	
Dissemination level	Public

Summary

This Data Management Plan (DMP) defines the principles, processes, and tools for handling data generated and used within the Digital Innovation Gateway for Kosovo (DIG-4K). It establishes guidelines for data collection, storage, documentation, sharing, and protection across the project's 48-month duration. The plan ensures compliance with relevant EU and national regulations,. It also identifies the types of data produced, responsible partners, data security measures, and access levels, while outlining procedures for long-term preservation. The DMP will be a living document, regularly updated to reflect project progress and emerging needs in data governance.

Disclaimer

Co-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 HaDea. Neither the European Union nor HaDea can be held responsible for them.

Contents

1. Introduction	6
1.1 Definitions	6
1.2 Purpose and Scope	7
1.3 Personal Data Categories.....	8
1.4 Who will have access to personal data	9
1.5 Third party access and data transfers outside the EEA	9
1.6 Data Retention Period.....	10
1.7 How personal data will be collected and processed	10
1.8 Customer Data for Service Provision	12
2. Description of Data Flows	13
2.1 Data Flow 1: Project Management and Coordination (WP1)	13
2.2 Data Flow 2: Digital Transformation Advisory Services (WP2).....	13
2.3 Data Flow 3: Digital Skills Academy (WP3).....	14
2.4 Data Flow 4: Tech Access and Testing Lab (WP4).....	14
2.5 Data Flow 5: Funding and Investment Support (WP5)	15
2.6 Data Flow 6: Ecosystem Development and Networking (WP6)	15
2.7 Data Flow 7: Upscaling, Exploitation, Communication, and Dissemination (WP7)	15
3. Datasets.....	17
3.1 Project Management and Coordination Dataset	17
Table 1.....	17
3.2 Digital Transformation Center-Advisory Services Dataset.....	17
Table 2.....	17
3.3 Digital Skills Academy Dataset.....	18
Table 3.....	18
3.4 Tech Access and Testing Lab Dataset.....	19
Table 4.....	19

3.5 Funding and Investment Support Dataset	19
Table 5.....	19
3.6 Ecosystem Development & Networking Dataset	20
Table 6.....	20
3.7 Upscaling, Exploitation, Communication, and Dissemination Dataset	20
Table 7	20
4. Security	21
4.1 Security Measures.....	21
5. Ethics.....	22

1. Introduction

This Data Management Plan (DMP) outlines a structured approach to the responsible handling, storage, and sharing of data within the DIG-4K project and its associated services. As the initial version, this DMP is considered a living document and will be revised as needed to support the entire data management lifecycle throughout the project's duration. It details data handling procedures up to and beyond the project's completion, including definitions of the types of data collected and processed.

The plan describes the methodologies and standards applied, with particular attention to data sharing, curation, and long-term preservation. DIG-4K is co-funded through the Digital Europe Programme, an EU funding programme focused on making Europe greener and more digital and by the government of Kosovo, through the Ministry of Economy. As part of the wider EDIH Network across Europe our mission is to empower Micro, Small, and Medium Enterprises (MSMEs), Public Sector Organizations (PSOs), and citizens to thrive in the digital age.

To execute all Work Package activities, DIG-4K will utilize, collect, and/or generate various types of data. This may include personal data, operational company data obtained from customers, bespoke data created within partner infrastructures (including research data), or open-source data stored in research facilities. The DIG-4K consortium prioritizes user privacy and data protection, adhering strictly to policies and principles that ensure compliance with applicable regulations.

All personal data will be processed in accordance with the EU General Data Protection Regulation (EU 2016/679, GDPR) as well as Law No. 06/L-082 on the Protection of Personal Data (2019) in Kosovo. This DMP sets out the main elements of the project's data management policy, including the procedures for collecting and handling personal data. Additionally, it defines the responsibilities of Data Controllers, establishes a joint controllers' framework for data sharing among partners, and specifies the purposes, legal basis, and nature of processing, the categories of personal data involved, and the retention periods applied.

1.1 Definitions

Throughout the DIG-4K project, the following definitions apply:

- **Data Controller:** The entity (organization or individual) which, alone or jointly with others, determines the purposes and means of processing personal data. In DIG-4K, this refers to ITP Prizren as the lead organization, together with relevant partners.
- **Joint Controllers:** According to Article 26(1) GDPR, where two or more controllers jointly determine the purposes and means of processing personal data, they shall be joint controllers. DIG-4K partners may act as joint controllers where applicable.
- **Data Provider:** The Party, acting as joint controller, whose role in the project involves the provision of personal data to DIG-4K, including transferring data to Data Recipients for purposes set out in the Grant Agreement.

- **Data Recipient(s):** The Party or Parties, acting as joint controllers, whose role in the project involves the processing, analysis, and use of personal data provided to DIG-4K by the Data Provider, in line with the project's objectives.
- **Data Processor:** A natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller.
- **Privacy and Data Protection Legislation:** Refers to the General Data Protection Regulation (GDPR; EU 2016/679), national data protection legislation, and all applicable laws related to personal data and privacy. This includes amendments to such laws over time.
- **Personal Data:** Personal data as defined in GDPR, which will be shared among project partners and detailed within this DMP.

1.2 Purpose and Scope

Processing of personal data is integral to delivering DIG-4K's services and activities. As per Article 4 of GDPR, processing refers to any operation performed on personal data, including collection, storage, retrieval, use, disclosure, and erasure.

Under DIG-4K, personal data processing will be strictly limited to purposes directly related to the project, including:

- Facilitation and delivery of project services and execution of service agreements.
- Providing access to training programs, innovation facilities, and digital transformation support.
- Enhancing user experience through tailored and customized service provision.
- Efficient management of networking and collaboration activities.
- Monitoring project progress, evaluating outcomes, and reporting impact.
- Analyzing trends and patterns to provide insights related to digital transformation.
- Dissemination and communication of project findings and results via newsletters, emails, and events.
- Production of promotional material (photos, videos, infographics, brochures) from events and service delivery.
- Engaging stakeholders in surveys, interviews, workshops, and other consultations.
- Responding to queries from participants and partners.

- Meeting legal and audit requirements, including reporting to EU bodies.
- Sharing necessary information with the European Commission (EC) and other authorized entities (e.g. Ministry of Economy) for monitoring and evaluation purposes.

Note: DIG-4K will not collect sensitive personal data (as defined by Article 9 GDPR, e.g., racial or ethnic origin, political opinions, religious beliefs, health data, etc.).

1.3 Personal Data Categories

In order to manage, execute, and implement DIG-4K services, a dataset containing personal data about professional contacts of participants from Micro, Small and Medium Enterprises (MSMEs), Public Sector Organizations (PSOs), startups, educational institutions, CSOs, and other organizations may be processed.

The categories of personal data processed include:

- **Identity Data:** First and last names, ID/passport numbers (where applicable for verification and reporting purposes), and gender data (for gender balance reporting).
- **Employment Data:** Proof of employed staff, including employment contracts or declarations to the Tax Administration of Kosovo (list of declared employees) when required to assess eligibility for services.
- **Business Registration Data:** Proof of business registration, including the Business Registration Number (NRB/NUJ), where necessary to confirm the legal status of the applicant organization.
- **Financial Data:** Proof of business turnover, including declarations to the Tax Administration of Kosovo or company financial statements, when needed to determine eligibility or tailor support services.
- **Contact Information:** Organization's address, work email, and telephone number.
- **Audiovisual Data:** Photos and videos of participants during events, training sessions, or service delivery, which may be used for reporting, dissemination, and promotional purposes across print and digital media (websites, social media, press releases etc.).

If, at any point, additional personal data not previously specified is required, DIG-4K will provide clear communication regarding:

- The type of data needed,
- The reasons for its necessity,
- Whether the provision of the data is mandatory, and

- The consequences of not providing the data.

1.4 Who will have access to personal data

Personal information gathered through user registration forms, surveys, event participation, and other project-related interactions will be received and processed by the data controllers of the DIG-4K project. Where required, personal data may also be accessed by other authorized members of the DIG-4K consortium, including researchers, administrative staff, and IT personnel, strictly for purposes of responding to requests, managing facility access, delivering services, and fulfilling project objectives.

Access to personal data will be restricted to authorized personnel only and protected through access controls (e.g., secure logins, encrypted repositories). Microsoft Teams, used as a communication and collaboration platform within the project, is subject to Microsoft's GDPR-compliant data processing agreements, and access to any personal data shared via Teams is similarly limited to authorized project members.

The DIG-4K data controllers are:

- Besmir Krasniqi, Innovation and Training Park (ITP) Prizren, besmir.krasniqi@itp-prizren.com
- Liridona Ahma, Innovation and Training Park (ITP) Prizren, liridona.ahma@itp-prizren.com
- Dea Mormorina, Innovation and Training Park (ITP) Prizren, dea.mormorina@itp-prizren.com
- Sedef Balik, Innovation and Training Park (ITP) Prizren, sedef.balik@itp-prizren.com
- Berat Abdiu, ALT SH.P.K, babdiu@alt-pr.com
- Vildane Kelmendi, Cactus Education, vildan.kelmendi@cactus.education
- Arbian Shkodra, Quantix LLC, arbian@thequantix.com
- Bardha Qirezi, Edutask, bardha.qirezi@edu-task.com
- Besnik Skenderi, University of Business and Technology (UBT), besnik.skenderi@ubt-uni.net
- Faruk Bojaxhi, University of Prizren Ukshin Hoti (UUHP), faruk.bojaxhi@uni-prizren.com
- Arber Kryeziu, Makerspace Innovation Center Prizren (MICP), arber@makerspaceprizren.com
- Valbon Kizolli, Kosovo Research and Education Network (KREN), valbon.kizolli@kren-ks.eu

DIG-4K's designated data protection contact person who will ensure compliance with data protection standards is Ms. Liridona Ahma.

1.5 Third party access and data transfers outside the EEA

Collected personal data will not be shared with third parties outside the consortium unless it is required to deliver project services or comply with legal obligations. In such cases, third parties will only process personal data under strict confidentiality and in accordance with GDPR.

Where DIG-4K relies on third-party IT service providers, subcontractors, or affiliated organizations to store or process data, contractual agreements will ensure they adhere to the same data protection obligations set out in this document and in line with Article 15 of the Grant Agreement.

Data may also be shared with the European Commission and other authorized entities as part of project monitoring and reporting requirements.

No transfers of personal data outside Kosovo and the European Union/European Economic Area (EU/EEA) will take place unless:

- the transfer is required by the project's contractual obligations with the European Commission,
- appropriate safeguards (e.g., Standard Contractual Clauses) are in place, and
- such transfer complies fully with GDPR requirements.

1.6 Data Retention Period

Personal data collected within DIG-4K will be retained only as long as necessary to achieve the purposes for which it was collected and to meet legal, accounting, or reporting obligations.

- Data will be actively used during the project implementation period.
- Following project completion, personal data may be securely archived for up to 5 (five) years after the end of the project or until consent is withdrawn.
- After this period, or upon a valid request for erasure, the data will be securely deleted or anonymized in compliance with GDPR and applicable national legislation.

DIG-4K adheres to the principle of data minimization, ensuring that only essential data is retained and that unnecessary data is promptly destroyed.

1.7 How personal data will be collected and processed

DIG-4K will implement the following measures to ensure compliance with applicable personal data protection requirements:

Compliance with Personal Data Processing Principles

Personal data processing under DIG-4K will follow the core principles outlined in GDPR:

1. Lawfulness, fairness, and transparency in all processing activities.
2. Data minimization – only data necessary for the project's objectives will be collected.
3. Purpose limitation – personal data will only be used for the purposes stated at the time of collection.

4. Accuracy – data will be kept up to date, with inaccurate information corrected or erased promptly.
5. Storage limitation – data will not be kept longer than necessary.
6. Integrity and confidentiality – appropriate security measures (technical and organizational) will protect data from unauthorized processing, loss, or destruction.

Compliance with National and EU Legislation

All personal data processing will be carried out in accordance with the General Data Protection Regulation (GDPR; EU 2016/679), as well as Law No. 06/L-082 on the Protection of Personal Data (2019) in Kosovo.

Informed Consent Procedures

Individuals whose personal data is collected will be clearly informed about:

- the type of data being collected,
- the purpose of processing,
- their rights under GDPR,
- and how to exercise these rights.

Consent will be obtained through appropriate mechanisms, such as checkboxes, signed forms, or digital confirmations. Project participants will also have access to the DIG-4K Privacy Policy, where all terms of data processing are explained.

Collection Methods

Personal data will be collected through:

- Expression of interest forms,
- Onboarding processes for training and innovation services,
- Digital maturity assessments (DMA),
- Event registrations, networking activities, and surveys,
- Newsletter sign-up forms, and
- Online tools (e-learning platforms)

Data Subject Rights

Individuals whose personal data is processed under DIG-4K have the right to:

- Information about how their data is used,
- Access to their personal data,
- Rectification of inaccurate data,
- Erasure ("right to be forgotten"),

- Restriction of processing,
- Data portability
- Object to processing, and
- Not be subject to decisions based solely on automated processing, including profiling.

To exercise these rights, data subjects may contact the Data Protection Contact Person of DIG-4K.

1.8 Customer Data for Service Provision

Under the DIG-4K project, data collected or generated during the provision of services (e.g., digital maturity assessments, advisory services, digital skills trainings, test before invest, access to funding, innovation ecosystem & networking) will remain the property of the customers (participating organizations or individuals). The data provider (customer) retains ownership and determines to what extent such data may be shared or reused, as well as any restrictions that apply.

The types of data that may be collected, processed, or generated include:

- **Observational Data:** Captured in real time during service delivery (e.g., event participation metrics, user interactions), typically cannot be reproduced exactly.
- **Experimental Data:** Generated from testing or pilot activities, which can often be reproduced.
- **Simulation Data:** Created through models or digital tools, reproducible if input data is known.
- **Derived or Compiled Data:** Produced after data analysis or processing (e.g., aggregated results from surveys, trend reports), reproducible if methodologies are documented.

Data collected during service provision will be handled exclusively by the DIG-4K partner responsible for delivering that specific service. It will not be shared with other consortium partners unless such sharing is necessary to fulfill project objectives.

Prior to providing any service, customers will be informed about:

- the type of data required,
- the conditions of data collection,
- the purpose of processing, and
- how the data will be stored, used, and protected.

This ensures transparency and consent in accordance with GDPR principles.

2. Description of Data Flows

The main data flows within DIG-4K result from the activities deriving from the following Work Packages (WPs):

- WP1 – Project Management and Coordination
- WP2 – Digital Transformation Centre – Advisory Services
- WP3 – Digital Skills Academy
- WP4 – Tech Access and Testing Lab
- WP5 – Funding and Investment Support
- WP6 – Ecosystem Development and Networking
- WP7 – Upscaling, Exploitation, Communication, and Dissemination

These WPs involve the collection and processing of data necessary for project management, delivering advisory services, training, testing, access to funds, ecosystem-building, communication and dissemination activities. Below is a summarized description of the data flows:

2.1 Data Flow 1: Project Management and Coordination (WP1)

The first data flow relates to project management, internal coordination, and reporting under WP1. DIG-4K processes data necessary to ensure smooth implementation of activities, compliance with EU funding requirements, and achievement of KPIs.

Data processed includes:

- contact details of project staff, consortium members, and stakeholders involved in project activities,
- monitoring and evaluation data used to track progress and prepare KPI reports,
- financial and administrative records required for audits and compliance reporting.

Access to this data is restricted to authorized project management personnel. Data is stored securely and processed strictly for project coordination, monitoring, and reporting purposes in line with GDPR and national legislation.

2.2 Data Flow 2: Digital Transformation Advisory Services (WP2)

This data flow concerns the advisory services delivered through the Digital Transformation Centre. In this phase, DIG-4K collects data from MSMEs, public sector entities, and other stakeholders to evaluate their digitalization status and provide tailored roadmaps.

Data processed includes:

- organizational information (sector, size, digital readiness level),
- needs assessments through questionnaires and consultations,
- and feedback data to refine advisory services.

This information enables DIG-4K to design customized digitalization strategies and improve the quality of advisory services provided. Access to customer data is essential for aligning recommendations with the specific needs and strategic goals of each organization.

2.3 Data Flow 3: Digital Skills Academy (WP3)

This data flow involves activities under the Digital Skills Academy, which provides tailored training programs for MSMEs, PSOs, and educational institutions.

Data collected includes:

- participant registration data (identity and contact information),
- pre- and post-training assessments,
- feedback on training quality and outcomes,
- and certification records.

This data allows DIG-4K to:

- identify skills gaps,
- customize training to participant needs,
- monitor learning outcomes, and
- ensure effective skills recognition.

All data is processed securely and used solely to enhance training effectiveness and impact.

2.4 Data Flow 4: Tech Access and Testing Lab (WP4)

This data flow pertains to the Tech Access and Testing Lab, where participants can access AI technologies, testing environments, and consultancy support.

Customer data processed in this phase may include:

- technical specifications of solutions being tested,
- usage data from lab facilities,

- and performance outcomes from tests.

This information helps DIG-4K tailor the testing environment to customer needs, provide expert guidance, and document results to mitigate risks before investment decisions are made.

2.5 Data Flow 5: Funding and Investment Support (WP5)

This data flow supports stakeholders in accessing funding and investment opportunities. This includes grant writing workshops, fundraising guidance, and matchmaking with investors.

Data processed includes:

- applicant profiles,
- funding needs assessments,
- and records of participation in events and matchmaking activities.

Such data is critical to align funding recommendations with the customer's strategic objectives and to track the effectiveness of investment support services.

2.6 Data Flow 6: Ecosystem Development and Networking (WP6)

This data flow relates to ecosystem development, networking, and partnership building. DIG-4K facilitates collaboration across local, regional, and European innovation ecosystems.

Data processed includes:

- contact information of ecosystem stakeholders,
- event participation records,
- and feedback data to improve networking initiatives.

This data enables DIG-4K to analyze innovation trends, identify opportunities, and tailor networking efforts to maximize the benefits for all ecosystem participants.

2.7 Data Flow 7: Upscaling, Exploitation, Communication, and Dissemination (WP7)

The last data flow concerns activities under WP7, which focus on promoting the project, scaling its impact, and disseminating results to relevant audiences.

Data processed in this phase includes:

- contact details of stakeholders subscribed to newsletters or mailing lists,
- event participation data (e.g., attendee lists, feedback surveys),
- photos and audiovisual content collected during events for dissemination purposes,

- website and social media analytics to measure outreach effectiveness.

All communications and dissemination activities comply with GDPR, ensuring that:

- consent is obtained where required (e.g., for newsletters subscription, use of photos),
- individuals are informed about the use of their data, and
- data is processed solely for the purposes of project communication and result exploitation.

3. Datasets

Datasets resulting from DIG-4K's data flows described in the previous section are presented here.

Each dataset table includes: dataset reference, relevant WP, description, data utility, origin, archiving and storage, and data sharing policy.

3.1 Project Management and Coordination Dataset

Table 1

Dataset reference	DIG-4K Dataset 1
Relevant WP	WP1
Description	Contact information of consortium members, project staff, and stakeholders; monitoring and evaluation data; KPI tracking records; financial and administrative data required for audits.
Data Utility	Used to coordinate project activities, prepare reports, and ensure compliance with EU and national requirements.
Origin	Internal project communication, KPI reports, attendance lists, financial documentation
Archiving and Storage	Stored in a secure Microsoft Teams project folder, accessible only to project management personnel
Data Sharing Policy	Internal

3.2 Digital Transformation Center-Advisory Services Dataset

Table 2

Dataset reference	DIG-4K Dataset 2
Relevant WP	WP2 – Digital Transformation Centre – Advisory Services
Description	Organizational data (sector, size, readiness level); contact data of representatives; needs assessment responses and feedback.

Data Utility	Supports provision of tailored advisory services, development of digitalization roadmaps, and refinement of services.
Origin	Expression of interest forms, digital readiness questionnaires, consultations
Archiving and Storage	Secure project storage (Microsoft Teams), accessible to relevant consortium members
Data Sharing Policy	Internal

3.3 Digital Skills Academy Dataset

Table 3

Dataset reference	DIG-4K Dataset 3
Relevant WP	WP3 – Digital Skills Academy
Description	Identity and contact data of training participants; pre/post-training assessment results; feedback surveys; certification records.
Data Utility	Used to customize training, evaluate learning outcomes, and issue certifications.
Origin	Registration forms, assessments, training evaluations
Archiving and Storage	Secure project storage (Microsoft Teams). Training data stored securely in project databases
Data Sharing Policy	Internal (certifications may be shared publicly with consent)

3.4 Tech Access and Testing Lab Dataset

Table 4

Dataset reference	DIG-4K Dataset 4
Relevant WP	WP4 – Tech Access and Testing Lab
Description	Technical specifications of solutions tested; usage logs; performance data; consultancy notes.
Data Utility	Enables tailored lab support, risk assessment, and documentation of testing outcomes.
Origin	Data submitted by participants during testing, lab-generated logs
Archiving and Storage	Secure project storage (Microsoft Teams), access limited to lab teams
Data Sharing Policy	Internal (results may be shared with customers under agreed terms)

3.5 Funding and Investment Support Dataset

Table 5

Dataset reference	DIG-4K Dataset 5
Relevant WP	WP5 – Funding and Investment Support
Description	Profiles of applicants seeking funding; funding needs assessments; participation records in grant writing workshops and matchmaking events.
Data Utility	Used to align funding support services, monitor outcomes, and report activities.
Origin	Registration forms, funding applications, event attendance lists
Archiving and Storage	Secure project storage (Microsoft Teams).
Data Sharing Policy	Internal (applicant data not shared externally without consent)

3.6 Ecosystem Development & Networking Dataset

Table 6

Dataset reference		DIG-4K Dataset 6
Relevant WP		WP6 – Ecosystem Development and Networking
Description		Contact details of ecosystem stakeholders; event attendance data; feedback surveys from networking sessions.
Data Utility		Facilitates building of the digital innovation ecosystem, trend analysis, and networking improvements.
Origin		Event registrations, stakeholder engagement forms
Archiving and Storage		Stored in project databases (Teams); restricted access to networking team
Data Sharing Policy		Mixed (event photos may be publicly shared; contact data is internal)

3.7 Upscaling, Exploitation, Communication, and Dissemination Dataset

Table 7

Dataset reference		DIG-4K Dataset 7
Relevant WP		WP7 – Upscaling, Exploitation, Communication, and Dissemination
Description		Stakeholder contact data for mailing lists; event participation data; audiovisual content (photos/videos); website and social media analytics.
Data Utility		Used for newsletters, promotional materials, monitoring outreach, and disseminating project results.
Origin		Newsletter subscriptions, event registrations, media captured during events.
Archiving and Storage		Stored in communication team repositories and MS teams; audiovisuals stored securely with controlled access
Data Sharing Policy		Mixed (photos/videos may be publicly available; personal contact data kept internal)

4. Security

Considering technological advancements, implementation costs, and the nature, scope, context, and objectives of data processing within the DIG-4K project, the consortium partners will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks, in accordance with GDPR Article 32 and best practices in cloud collaboration platforms.

- All communication, document sharing, and collaboration within the project is conducted primarily through Microsoft Teams and Microsoft 365. The following security measures apply:

4.1 Security Measures

- User Authentication
 - All users accessing Microsoft Teams or associated Microsoft 365 services (e.g., SharePoint, OneDrive) must authenticate using their approved institutional accounts.
 - Multi-Factor Authentication (MFA) is required for all users.
- Access Control
 - Access to project resources is strictly limited to authorized consortium members.
 - Team owners must regularly review membership lists and permissions.
 - Any user no longer involved in the project will have their access revoked immediately.
- Storage Security
 - Documents must be stored within Microsoft Teams channels or connected SharePoint repositories.
 - Downloading files to personal or unsecured devices is strongly discouraged unless necessary.
- Where applicable:
 - Electronic files must be password-protected.
 - Data at rest is encrypted by Microsoft 365 services.
- Communication Security
 - All communication within MS Teams (chat, calls, video conferences) is end-to-end encrypted.
 - External sharing of data or links outside the consortium must be explicitly authorized.
 - Devices used to access project systems must have:

- Updated antivirus/anti-malware protection.
 - Active firewall configuration.
- Physical Device Security
 - Laptops, mobile phones, and desktops used to access DIG-4K resources must be secured with passwords or biometric locks.
 - Devices must be locked or logged off when unattended.
 - Physical transfer of data carriers (e.g., USBs, printed notes) should be avoided. If necessary, they must be securely transported.
- Other IT Controls
 - Operating systems and software must be regularly updated with security patches.
 - Unauthorized installation of applications on work devices is prohibited.
 - Local backups, if used, must be encrypted and stored securely.

Additional Recommendations

- Avoid downloading or storing documents locally; use cloud storage within the Microsoft 365 environment.
- Do not share credentials or authentication codes with others.
- Report any suspected security incidents or unauthorized access to the project IT security contact immediately.

Access Management

- Access to Microsoft Teams channels, files, and repositories is granted strictly based on project role and necessity. Any changes in team member status must be reflected in the access control list without delay.

5. Ethics

The processing of personal data under the DIG-4K project is not subject to the approval of ethics committees or public authorities. However, all data processing strictly adheres to:

- the General Data Protection Regulation (GDPR),
- Law No. 06/L-082 on the Protection of Personal Data (2019) in Kosovo.
- and ethical principles of transparency, fairness, and accountability.

All personal data is collected and processed lawfully, ensuring respect for individuals' rights to privacy and data protection.