



Higher Education and Science Information Technology Shared Service Centre

Project Charter

EOSC Node Latvia

1. PROJECT SUMMARY

The Higher Education and Science Information Technology Shared Service Centre (VPC), acting as Latvia's EOSC Mandated Organisation, will create and operate the EOSC Node Latvia as the national gateway to the EOSC Federation. This project charter defines the activities and resources required to realise this Node.

The primary purpose of Latvia's participation is to advance Open Science by integrating national research data, services, and expertise into a federated European ecosystem. This enables cross-border access to FAIR data and services, fosters collaboration, and supports reproducible, data-intensive research across disciplines and borders.

The project has a national and multidisciplinary scope, covering research-performing organisations and infrastructures across Latvia. Through EOSC Node Latvia, these organisations and resources will be connected to the EOSC Federation and its shared capabilities, supporting research in areas such as health and genomics, climate and biodiversity, energy, agriculture, language technologies and socio-economic research.

The main goal is to establish an operational EOSC Node Latvia with core federating capabilities and to onboard Latvian repositories and services. This will make Latvian research outputs and digital services discoverable and usable through the EOSC EU Node and other EOSC Nodes. The Node addresses the need for secure, standards-based access to high-value FAIR data, interoperable services, and federated research environments for Latvian and European researchers.

Key resources made available to the Federation include federated authentication and authorisation integrated with EOSC AAI, high-speed research network connectivity and large file transfer services, interactive notebooks and compute environments for data analysis, and File Sync & Share for collaborative research.

A National Service Catalogue will be registered with the EOSC EU Node Resource Catalogue, aggregating metadata from DataverseLV, RSU Dataverse and other providers so their research products and services can be discovered and used through the EOSC Federation.

2. VALUE PROPOSITION

EOSC Node Latvia addresses key gaps in the EOSC ecosystem by extending geographical coverage, integrating fragmented national infrastructures, and providing federated, standards-based services for data-intensive research. It tackles the following challenges and needs:

- **Lack of national-level coordination and aggregation:** data infrastructures, thematic repositories, and digital services in Latvia are scattered across institutions. EOSC Node Latvia establishes a national coordination hub that federates these resources and connects them to the EOSC Federation.
- **Limited capacity for secure large-scale data exchange:** the existing academic network is outdated and cannot fully support modern data-intensive workflows. The Node will modernise the national research network with high-speed, research-only connectivity and large file transfer services, enabling cross-border collaboration.
- **Low EOSC-wide visibility of Latvian research outputs:** Latvian data and services are not systematically exposed to EOSC Federation. A central metadata registry and

service catalogue will integrate Latvian repositories and services into EOSC resource catalogue for Europe-wide discovery and reuse.

- **Gaps in trusted identity and access management:** Latvian researchers require seamless, secure access to EOSC resources. EOSC-compliant AAI, based on the Latvian Academic Federation and eduGAIN and interoperable with EOSC AAI, will provide single sign-on across nodes.
- **Growing cybersecurity and compliance obligations:** institutions must meet NIS2, GDPR and national requirements. EOSC Node Latvia will implement federation-aligned cybersecurity measures and support connected institutions in achieving compliance.

Beneficiaries include:

- **Researchers**, who gain secure access to Latvian and European data, computing, storage, and federated research environments.
- **Research institutions and universities**, which will benefit from shared infrastructure, reduced duplication, improved compliance, and stronger capacity to participate in Horizon Europe and future Framework Programme projects.
- **Private sector and industry**, which can access research data and secure data-sharing infrastructures for innovation and R&D collaboration.
- **Citizens and society**, who benefit from greater transparency and access to publicly funded research outputs.

VPC's unique value lies in its national mandate, its role in serving the whole Latvian research ecosystem, its operation of shared national infrastructure, and its expertise in research data management through coordination of the national Data Stewards network and operation of the national research data repository DataverseLV. EOSC Node Latvia will serve as Latvia's main integration point to the EOSC Federation.

3. REPOSITORIES AND SERVICES DELIVERED

Service ID	Service Description	Access Policies to the Service	Federation Contributions & Value to Users	TRL
LV-S-1	DataverseLV - Latvian National Research Data Repository.	Data deposit open to researchers from Latvian scientific institutions. Datasets may be open or restricted according to depositor requirements.	Provides a national, multidisciplinary repository where Latvian researchers can deposit and publish datasets, while exposing metadata to the EOSC Federation.	8
LV-S-2	RSU Dataverse - Institutional repository of Rīga Stradiņš University.	Deposit primarily for RSU researchers and collaborators. Open access to non-sensitive datasets and controlled access to	Provides a dedicated repository for institutional medical and social science research data while exposing metadata to the EOSC Federation.	8

		sensitive data.		
LV-S-3	FileSender - secure large file transfer service.	Available to authenticated users via eduGAIN-compatible institutional identities.	Provides researchers with a secure mechanism for transferring large files and supports data-intensive research workflows through EOSC Node Latvia.	8
LV-S-4	NextCloud - cloud service for secure file synchronisation, sharing and team collaboration	Available to authenticated users via eduGAIN. With access control at project and institutional level.	Provides a shared File Sync & Share capability to the EOSC Federation and its users.	7
LV-S-5	National metadata catalogue - aggregating descriptions of Latvian research datasets and services.	Metadata open for search and harvest to the public.	Provides the Node Core “Resource Catalogue & Registry” capability by exposing aggregated Latvian dataset and service metadata to the EOSC Federation, giving users one place to discover Latvian research resources.	7
LV-S-6	EOSC Competency Centre - National support and training hub	Training materials and general guidance will be openly available where possible. Consultations and specialised support will be provided according to the applicable service and user-support arrangements.	Node Core Capability for “Helpdesk and Support” helping users use EOSC Federation services effectively.	7
LV-S-7	Interactive Notebooks - integrated with storage and compute.	Available to authenticated users via eduGAIN	Provides an interactive compute capability to the EOSC Federation and its users.	7

4. USE CASES

Use Case ID	Use Case Description	Federation Contributions & Value to Users	List of the participating organisations	List any other Nodes involved	Timeline of realisation of the use case
LV-UC-1	High-Speed Data Transfer. Secure and efficient transfer of large research datasets between Latvian research institutions and external research facilities or collaborators using FileSender and the Latvian Academic and Research Network.	Value: Enables researchers to transfer large datasets securely and efficiently between Latvian research institutions and external collaborators Contribution: Demonstrates how high-speed national research-network connectivity and FileSender can support the EOSC Connectivity layer and data-intensive research workflows.	- VPC (Service manager) - 26 Research institutions in Latvia	-	Prototype: M8 (12/2026) Production: M14 (06/2027)
LV-UC-2	Federated File Sync & Share. Provision of secure shared workspaces through the Nextcloud service of EOSC Node Latvia, using federated institutional authentication for access by	Value: Simplifies collaboration; removes the need for multiple accounts; ensures data sovereignty and GDPR compliance. Contribution: Demonstrates	- VPC (Service manager) - 26 Research institutions in Latvia	- EOSC Node SURF	Prototype: M12 (04/2027) Production: M20 (12/2027)

	researchers from participating institutions	how federated authentication can support research collaboration through a national EOSC Node service.			
LV-UC-3	Federated discovery of Latvian research data. Demonstrates how federated authentication can support research collaboration through a national EOSC Node service.	Value: Provides a common point for discovering Latvian research data through the EOSC Federation. Contribution: Demonstrates federated discovery by combining repository metadata and services from EOSC Node Latvia and the EGI Node.	- VPC (Coordinator and DataverseLV) - RSU (RSU Dataverse)	- EOSC Node EGI	Prototype: M6 (10/2026) Production: M14 (06/2027)
LV-UC-4	Embedding Open Science Competence Centres into EOSC Nodes. Development and testing of a shared approach for integrating training, guidance, onboarding and community-support functions into national EOSC Node operations.	Value: Connects technical Node development with the training and support required by researchers and institutions. Contribution: Produces practical examples and guidance that may support similar competence-centre functions in other EOSC Nodes.	- FCSE (MK), - PG (PL), - VPC (LV)	- EOSC Node North Macedonia, - EOSC Node Poland	Prototype: M8(12/2026) Production: M14 (06/2027)

LV-UC-1: High-Speed Data Transfer for Data-Intensive Research

- **Extended Use Case Description:** Latvian researchers working in data-intensive research fields may need to transfer terabytes of experimental data to their home institutions for processing and analysis.
This use case will provide access to the FileSender service operated by EOSC Node Latvia over the upgraded Latvian Academic and Research Network. It will test secure and efficient transfer of large datasets between external research facilities and selected Latvian institutions, particularly in fields such as solid-state physics, biophysics, crystallography, omics and organic synthesis.
- **Value Proposition:** The use case will reduce transfer times and provide researchers with a secure alternative to commercial file-sharing services with limited file size, storage or performance.
It will also demonstrate how FileSender and high-speed research-network connectivity can support the EOSC Connectivity layer and data-intensive scientific workflows.
- **In Scope:**
 - (a) **Research scenarios:** Identification and testing of representative data-transfer workflows involving Latvian researchers working with other data-intensive research infrastructures.
 - (b) **High-speed data transfer:** Transfer of large research datasets through the upgraded Latvian Academic and Research Network.
 - (c) **FileSender Service:** Deployment and testing of FileSender as the user-facing service for secure large-file transfer.
 - (d) **Authentication and Access:** Access to the service for authenticated researchers through eduGAIN-compatible identity services.
 - (e) **Performance Testing:** Assessment of transfer speed, stability, reliability and file-size handling under representative research conditions.
 - (f) **Support:** Preparation of user documentation and support for participating researchers and institutions.
 - (g) **Pilot Evaluation:** Collection of feedback and documentation of the technical and operational lessons identified during implementation.
- **Out of Scope:**
 - (a) **Excluded Activities:** The use case will not develop a new large-file transfer platform, network protocol or data-storage system. It will deploy and configure existing FileSender technology and use the infrastructure of the Latvian Academic and Research Network.
 - (b) **Limitations:** The initial pilot will focus on selected Latvian research institutions and representative data-intensive research scenarios. It will not cover all scientific disciplines or every possible external research facility during the build-up phase.
 - (c) **Data Processing:** The use case will support data transfer but will not itself provide scientific data analysis, long-term preservation or workflow-execution services.
 - (d) **Sensitive Data:** Transfers involving personal, confidential or otherwise sensitive data may require additional legal, security and organisational measures and will only be included where the necessary safeguards are available.
 - (e) **Dependencies:** Implementation will depend on the availability of the upgraded Latvian Academic and Research Network, the operational deployment of FileSender, eduGAIN-compatible authentication, suitable pilot researchers and cooperation with the relevant external research facilities.
- **Role of the Involved Organisations:**
 - (a) **EOSC Node Latvia/VPC:** Deploy and operate FileSender; provide high-speed network connectivity, authentication integration, service monitoring, user documentation and technical support; coordinate pilot implementation and evaluate the results.
 - (b) **Participating Latvian research institutions:** Identify representative research workflows and pilot users; participate in transfer testing; provide feedback on performance and usability; and support coordination with the relevant European research facilities.

LV-UC-2: File Sync & Share for Research Collaboration

- **Extended Use Case Description:** Latvian researchers need secure shared workspaces for exchanging documents, datasets and other research outputs within collaborative projects. Existing arrangements may require separate local accounts, fragmented institutional storage or the use of commercial file-sharing platforms.
This use case will provide a Nextcloud-based File Sync & Share service through EOSC Node Latvia. Researchers from participating institutions will be able to access shared project folders using federated institutional authentication, without requiring separate local accounts where compatible identity services are available.
Selected research teams will test user onboarding, access management, file sharing, synchronisation and collaboration through shared workspaces. The pilot will identify the technical, operational and user-support requirements for providing the service across Latvian research institutions.
- **Value Proposition:** The use case will provide researchers with a secure collaboration environment operated through trusted national research infrastructure.
It will simplify access to shared project spaces, reduce reliance on commercial platforms and demonstrate how federated authentication can support collaboration between researchers from different institutions.
- **In Scope:**
 - (a) **Shared workspace:** Provision of project folders and collaboration spaces through the Nextcloud service of EOSC Node Latvia.
 - (b) **Federated authentication:** Access through compatible institutional identities using LAIFE and eduGAIN.
 - (c) **Access management:** Testing user invitations, permissions, group membership and removal of access when collaboration ends.
 - (d) **Pilot activities:** Testing selected research collaboration scenarios involving participating Latvian institutions.
 - (e) **User support:** Preparation of basic guidance and support procedures for researchers and institutional administrators.
 - (f) **Pilot evaluation:** Collection of feedback and documentation of technical, operational and usability findings.
- **Out of Scope:**
 - (a) **Excluded Activities:** The use case will not develop a new File Sync & Share platform or replace institutional document-management and long-term data-preservation systems.
 - (b) **Limitations:** The initial pilot will involve selected research teams and institutions whose identity systems are compatible with the service.
 - (c) **Sensitive Data:** Sensitive or restricted data requiring specialised processing environments or additional legal and security safeguards will not be included in the initial implementation.
 - (d) **Cross-Node Federation:** Direct interoperability with File Sync & Share services operated by other EOSC Nodes will not be part of the initial implementation, but may be added later.
 - (e) **Dependencies:** Implementation will depend on the operational availability of the Latvian Nextcloud service, federated authentication, suitable pilot teams and the participation of relevant institutional IT staff.
- **Role of the involved organisations:**
 - (a) EOSC Node Latvia/VPC: Deploy and operate the Nextcloud service, integrate federated authentication, coordinate pilot activities, provide technical and user support, and document the results.

- (b) Participating Latvian research institutions: Identify suitable collaboration scenarios and pilot users, support testing, and provide feedback on access, usability and support needs.

LV-UC-3: Federated discovery of Latvian research data

- **Extended Use Case Description:** Latvian research data are distributed across national and institutional repositories and are not yet consistently discoverable through the EOSC Federation. This use case will build on the existing aggregation of metadata from DataverseLV and RSU Dataverse in the EGI Node through the EOSC Data Commons services ([EOSC Matchmaker](#) and [EOSC Data Player](#)). It will test how the EGI Matchmaker service can support the registration and federated discovery of these resources.
- **Value Proposition:** Providing researchers with a single point for discovering Latvian research data available through the EOSC Federation. The use case will increase the visibility and reuse of Latvian research outputs while demonstrating the added value of combining services from multiple EOSC Nodes.
- **In Scope:**
 - (a) **Stakeholder Support:** LV-UC-3 will support Latvian repository operators and researchers in making research data discoverable and reusable through the EOSC Federation.
 - (b) **Catalogue Integration:** Metadata from DataverseLV and RSU Dataverse will be aggregated and validated. The EOSC Data Commons service will be tested for registering Latvian services and research products.
- **Out of Scope:**
 - (a) **Excluded Activities:** LV-UC-3 will not develop new catalogue, repository, notebook or workflow-management software.
 - (b) **Limitations:** The initial implementation will cover DataverseLV and RSU Dataverse. Restricted or sensitive datasets requiring additional access procedures will not be included.
 - (c) **Dependencies:** The use case depends on the availability of suitable open datasets, stable repository interfaces, and the EOSC Data Commons catalogue software.
- **Role of the involved Nodes:**
 - (a) **EOSC Node Latvia:** Provide metadata from DataverseLV and RSU Dataverse; support metadata mapping and validation.
 - (b) **EGI Node:** Support the aggregation and discovery of Latvian research resources through the EGI Matchmaker service developed by the EOSC Data Commons project.

LV-UC-4: Embedding Open Science Competence Centres into EOSC Nodes

- **Extended Use Case Description:** National EOSC Nodes require training, guidance and user support alongside technical services. This use case will explore how Open Science support structures in Poland, North Macedonia and Latvia can contribute to the activities of their national Nodes. The participating Nodes will exchange experience, identify areas for cooperation and test selected forms of coordinated support. The work may include training, onboarding, guidance materials, community engagement and links between national support networks and EOSC Node services, to identify approaches that other Nodes could adapt.
- **Value Proposition:** The use case will provide an opportunity to connect technical Node development with the support activities needed by researchers and institutions.

It may help the participating Nodes improve coordination between service providers, trainers, data stewards and other support personnel. The resulting examples and guidance could also help other EOSC Nodes consider how similar support functions might be organised in their own national context.

- **In Scope:**
 - (a) **National support structures:** Review of how competence centres, data steward networks, training providers and related support structures may contribute to EOSC Node activities.
 - (b) **Exchange of experience:** Sharing of approaches to researcher training, user guidance, service onboarding and community support.
 - (c) **Pilot activities:** Testing of selected support or training activities involving the participating Nodes.
 - (d) **Joint outputs:** Preparation of practical guidance, examples or templates based on the experience of the three Nodes.
- **Out of Scope:**
 - (a) **Excluded Activities:** The use case will not create a shared international competence centre or replace national training and support arrangements.
 - (b) **Limitations:** The work will be based on selected activities and national examples from the participating Nodes. The results may therefore require adjustment before being applied elsewhere.
 - (c) **Dependencies:** Implementation will depend on the availability of relevant staff, existing training and guidance resources, and suitable opportunities for piloting the proposed activities.
- **Role of the involved Nodes:**
 - (a) **EOSC Node North Macedonia:** Contribute experience from its Open Science Centre, training platform and national Open Science community, and take part in the pilot activities.
 - (b) **EOSC Node Poland:** Contribute experience from national Open Science training, competence-centre activities and support resources, and participate in developing the joint outputs.
 - (c) **EOSC Node Latvia:** Contribute experience from research data management support, institutional training and the Latvian Data Stewards Network, and take part in testing and reviewing the proposed approach.

5. COMPLIANCE WITH TECHNICAL REQUIREMENTS

EOSC Node Latvia confirms its commitment to comply with the mandatory technical specifications of the EOSC Federation, including the EOSC Interoperability Framework and Rules of Participation. The Node will implement the mandatory Federating Capabilities for authentication and authorisation, resource cataloguing and registration, helpdesk, monitoring and service management to support integration with the EOSC EU Node and other Federation members.

Governance Structure

EOSC Node Latvia will be hosted by the Higher Education and Science Information Technology Shared Service Centre (VPC), Latvia's EOSC Mandated Organisation and operator of the Latvian Academic and Research Network. VPC will act as the legal Node Host on behalf of the Ministry of Education and Science and will sign the EOSC Federation Memorandum of Understanding.

The Node will be led by a Coordinator, supported by an Operations Officer responsible for the Node Operations Team and the day-to-day coordination of technical operations and EOSC integration. A Cybersecurity Officer, Legal and Procurement Officer, and Communications Officer will support compliance with the EOSC Rules of Participation, legal and cybersecurity requirements, and communication with national stakeholders and EOSC governance bodies.

Strategic oversight will be provided by an Advisory Board representing Latvia's four major research universities: RTU, LU, RSU and LBTU. Long-term investment and implementation capacity are supported through ERDF-funded Project No. 1.1.1.6/1/25/I/001, implemented by VPC, with funding secured until November 2029.

Technical readiness

The Node will build on the upgraded Latvian Academic and Research Network, with a planned 1.6 Tbit/s core and 100G/400G connections to more than 26 research institutions. This infrastructure will support high-capacity connectivity for data-intensive research and the delivery of services such as FileSender and File Sync & Share.

Compute and secure processing environments will use production-grade infrastructure and established software components. Services made available through the Node will be deployed at the maturity level required for reliable pilot or production use, in accordance with the implementation schedule set out in this charter.

Integration in the EOSC Federated AAI

EOSC Node Latvia will integrate into the EOSC AAI Federation by leveraging the national identity federation (LAIFE) and eduGAIN, which VPC operates as the national NREN operator.

A national AAI proxy will connect Latvian services with the EOSC Federation and enable federated single sign-on and controlled access to Node services. Where applicable, access will be supported through EOSC-compatible identity and access-management solutions, including MyAccessID.

Access requirements and assurance levels will be determined according to the risk profile and access policy of each service. VPC will support participating institutions in meeting the necessary identity-assurance requirements through technical guidance and training.

Exposure of Resources through the EOSC Catalogue

The Node will expose Latvian research resources through a national metadata aggregator connected to the EOSC Resource Catalogue. The initial implementation will harvest metadata from DataverseLV and RSU Dataverse, with other repositories considered for subsequent onboarding.

- Provide an OAI-PMH endpoint compliant with the "Registration of EOSC Research Product Catalogues" guideline and the EOSC Research Product Profile.
- Map local metadata to DataCite 4.5 and DCAT-AP 2.1.1 profiles to ensure semantic interoperability with the EOSC EU Node.
- Synchronise regularly with the EOSC EU Node so that newly deposited datasets in Latvian repositories appear promptly in the central EOSC catalogue

Implementation of Node Core Capabilities

EOSC Node Latvia will implement all Node Core Capabilities as described in the EOSC Federation Handbook:

- **Resource Catalogue & Registry:** a national metadata aggregator as Node Core catalogue, exposing Latvian datasets and services to the EOSC Resource Hub.
- **AAI:** an AARC Blueprint-aligned architecture, providing federated access to Node Core and Node Exchange services.
- **Helpdesk:** an EOSC Node Latvia helpdesk at VPC, integrated with the EOSC Federation Helpdesk.
- **Monitoring:** A unified monitoring system will continuously check the health, availability and reliability of Node services and publish standard metrics, using EOSC-compatible tools, such as ARGO, where appropriate.
- **FitSM-based Service Management System:** A lightweight service management system aligned with FitSM to ensure structured, interoperable service planning, delivery, and continual improvement across the Node.

Cybersecurity framework and NIS2 compliance

The EOSC Node Latvia will operate under an information security management framework aligned with ISO/IEC 27001 for key assets (LAT network, storage, AAI), in line with NIS2 obligations for essential entities and with EOSC security recommendations.

ITSRM² will be used to perform regular risk assessments, ensuring systematic treatment of threats and vulnerabilities. VPC will establish a dedicated CSIRT function for the Node, coordinating with CERT.LV and the EOSC Security Coordination Group on incident response and cross-border security events.

6. EXTERNAL DEPENDENCIES & KEY RISKS

External Dependencies & Risks	Actions/mitigations measures	Deadline
Funding and cost pressures: Cost increases, procurement changes or unforeseen implementation needs may affect the available project budget.	Risk is mitigated by secured ERDF Project No. 1.1.1.6/1/25/I/001 with a total budget of €16.74M committed until Nov 2029, including a dedicated €2.7M reserve for infrastructure equipment. Mitigation includes real-time budget monitoring, multi-level financial oversight, and regular review meetings to align procurement with project phases.	During the project
Delays in Project Implementation: Deviations from the planned timeline due	Detailed work planning, monthly progress reviews, early risk detection, corrective action procedures, and formal change	During the project

to technical, organisational, or procurement delays.	management for timeline adjustments.	
Dependencies on EOSC Federation services and partner Nodes: Implementation of AAI, catalogue integration, federated discovery and joint use cases depend on the availability and technical readiness of EOSC Federation services and participating Nodes.	Joint work plans and implementation timelines will be agreed with the relevant partners. Alternative sequencing or reduced pilot scope will be used where external services or partner contributions are delayed.	During the project
Institutional readiness and user participation: Participating institutions may have different levels of technical readiness, identity-assurance capability, staff capacity and willingness to join pilot activities.	Early engagement with institutional IT teams, repository managers, data stewards and pilot users; provision of technical guidance, onboarding support and test environments; phased participation where necessary.	During the project
Regulatory and Policy Changes: New EU or national regulations (e.g., NIS2, AI Act, Data Spaces regulations) requiring redesign of services.	Active participation in EOSC and GEANT working groups, modular service architecture, compliance monitoring, and contingency prioritisation plans.	During the project
Cybersecurity and Data Protection Risks: Security breaches or non-compliance with GDPR/NIS2 or national requirements may affect Node services and users.	Security-by-design architecture, regular audits, incident response procedures, and dedicated IT security experts	During the project
Service interoperability and performance risks: Differences between institutional systems, metadata interfaces, identity services or network configurations may affect interoperability, transfer performance or service	Technical testing, validation in pilot environments, performance monitoring, documentation of limitations and phased deployment before production release.	During the project

reliability		
-------------	--	--

7. CONTRIBUTIONS [DELIVERABLES (INCLUDING DOCUMENTATION)]

Deliverable ID	Deliverable Name	Responsible	Deadline
LV-DEL-1	Updated Project Charter incorporating cross-Node use cases	VPC	M3 – July 2026
LV-DEL-2	EOSC Federation-compliant Node AAI proxy integrated with the national LAIFE eduGAIN infrastructure and validated through AARC-G052 and AARC-G069 tests	VPC	M6 – October 2026
LV-DEL-3	Operational Node Resource Catalogue registered in the EOSC EU Node Catalogue	VPC	M10 – February 2027
LV-DEL-4	Operational Service Helpdesk System	VPC	M12 – April 2027
LV-DEL-5	Operational FileSender service on the Latvian Academic and Research Network	VPC	M14 – June 2027
LV-DEL-6	Operational federated discovery of Latvian research data through EGI Data Commons	VPC, RSU and EGI Node	M14 – June 2027
LV-DEL-7	Operational National EOSC Competence Centre with an initial	FCSE (MK), PG (PL), VPC (LV)	M14 – June 2027

	training and guidance programme		
LV-DEL-8	Operational Nextcloud-based File Sync & Share service	VPC	M20 – December 2027

8. COMMUNITY ENGAGEMENT

Confirmation of Capacity

The VPC, acting as Latvia's designated EOSC Node operator, confirms its capacity and commitment to implement comprehensive community engagement activities across the entire Latvian research ecosystem.

Backed by funded project resources [Project No. 1.1.1.6/1/25/I/001] and VPC members from Latvia's four largest research universities (RTU, LU, RSU, LBTU). VPC has secured the organizational, financial, and human resources to establish a Competence Centre with dedicated staff for training, helpdesk, and policy support.

Our governance model, endorsed by the Ministry of Education and Science, positions VPC as the national bridge - ensuring researchers, institutions, and third-party service providers across Latvia can not only access but actively contribute to the EOSC Federation.

Enabling Community Participation

Local Knowledge Transfer (EOSC LV Technology Days): to ensure sustainable competence-building in Latvia, we will organise “EOSC LV Technology Days” targeting service administrators and network engineers, as well as thematic workshops for researchers and service providers. These events will facilitate direct knowledge transfer on critical topics such as AAI integration, service monitoring, and compliance with the EOSC Interoperability Framework.

Latvia's Data Stewards Network: embedded within the four major universities (RTU, LU, RSU, LBTU) and VPC, will support researchers from all Latvian research institutions in developing EOSC capabilities. They will act as the primary educators, teaching researchers how to manage data in accordance with FAIR principles, implement Open Science workflows in practice, and utilise EOSC Node services. This approach ensures sustainable, discipline-specific competence multiplication across the entire Latvian research ecosystem.

Onboarding of Latvian Institutions and Resources

EOSC Node Latvia will develop the capacity to onboard resources and services from up to 26 Latvian research institutions by 2029.

Standardised onboarding: Resource providers will receive an onboarding guide, technical requirements and access to a test environment where interoperability can be validated before production onboarding.

Policy support: Templates and guidance related to access policies, service descriptions and the EOSC Rules of Participation will be provided to reduce administrative barriers, particularly for smaller institutions.

Pilot participation: Selected research teams and service providers will be invited to test Node services and provide feedback before wider production deployment.

Community-Engagement Approach

EOSC Node Latvia will embed community engagement into Node development and operation through training, consultations, pilot activities, usability feedback and targeted communication.

Drawing on experience from first-wave EOSC Nodes and the EOSC EU Node, the approach will focus on:

- continuous engagement through the National EOSC Competence Centre and EOSC LV Technology Days;
- clear onboarding procedures, technical guidance and pilot testing;
- participation of major Latvian universities and other research institutions in identifying user needs and informing Node priorities.

9. TIMING AND MILESTONES

ID	Milestone Description	Target Delivery Date
LV-MS-1	Project initiated, Project charter developed	M1 – May 2026
LV-MS-2	National and cross-Node use-case scopes and implementation timelines defined	M3 – July 2026
LV-MS-3	Metadata from DataverseLV and RSU Dataverse made discoverable through an initial EGI Data Commons integration	M6 – October 2026
LV-MS-4	EOSC Federation-compliant Node AAI proxy operational and validated through AARC-G052 and AARC-G069 tests	M6 – October 2026
LV-MS-5	FileSender and National EOSC Competence Centre prototypes available	M8 – December 2026

LV-MS-6	Node Resource Catalogue operational and registered in the EOSC EU Node Catalogue	M10 – February 2027
LV-MS-7	EOSC Node Latvia Helpdesk operational and File Sync & Share prototype available	M12 – April 2027
LV-MS-8	FileSender service, federated discovery through EGI Data Commons and National EOSC Competence Centre platform operational	M14 – June 2027
LV-MS-9	Nextcloud-based File Sync & Share service operational	M20 – December 2027

10. CONTACTS

The project currently employs staff members as listed below. In total, more than 30 professionals will be engaged in the establishment of the EOSC Node Latvia, each specialising in their respective field to ensure the successful creation of the Node.

Role	Name	Email
Coordinator	Ilja Afanasjevs	ilja.afanasjevs@vpc.lv
Deputy Coordinator	Mikus Melderis	mikus.melderis@vpc.lv
Operations Officer	Kristaps Oškalns	kristaps.oskalns@vpc.lv
Cybersecurity Officer	Sarmīte Daņilova	sarmite.danilova@vpc.lv
Legal/procurement Officer	Sandra Jurago	sandra.jurago@vpc.lv
Communications Officer	1. Rebeka Birziņa 2. Inese Jaudzema	1. Rebeka.birzina@vpc.lv 2. Inese.Jaudzema@vpc.lv