eosc | Tripartite

Higher Education and Science Information Technology Shared Service Centre

Project Charter

EOSC Latvia Node

Last update: 10/10/2025

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 Latvia Node 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 that enables seamless 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 and connecting them, via the EOSC Latvia Node, to the EOSC Federation and its shared services in domains 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 Latvia Node with core federating capabilities and to onboard Latvian repositories and services so that their research outputs become 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, CLARIN-LV and other providers so their research products and services can be discovered and used through the EOSC Federation.

2. VALUE PROPOSITION

EOSC Latvia Node 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 Latvia Node 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 (MyAccessID), will provide single sign-on across nodes.
- Growing cybersecurity and compliance obligations: institutions must meet NIS2 and national requirements. The Node will implement federation-aligned cybersecurity measures and support connected institutions in achieving compliance.

Beneficiaries include:

- Researchers, who gain secure, FAIR-compliant access to Latvian and European data, computing, storage, and federated research environments.
- Research institutions and universities, which 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 Latvia Node 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 sensitive data.	Provides a dedicated repository for institutional medical and social science research data while exposing metadata to the EOSC Federation.	8
LV-S-3	CLARIN-LV - repository with Latvian, Latgalian and Livonian language resources.	Open access for researchers, language technologists, students.	Supplies curated Latvian, Latgalian and Livonian language corpora, lexical resources to the EOSC catalogue, enabling researchers across the Federation to use these resources.	8
LV-S-4	FileSender - secure large file transfer service.	Available to authenticated users via eduGAIN.	Provides a large-file transfer capability for EOSC Federation and its users.	8
LV-S-5	NextCloud - cloud service for secure	Available to authenticated users	Provides a shared File Sync & Share capability to	7

	file synchronisation, sharing and team collaboration	via eduGAIN. With access control at project and institutional level.	the EOSC Federation and its users.	
LV-S-6	Central 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-7	EOSC Competency Centre - National support and training hub	Available to all EOSC Federation authenticated users.	Node Core Capability for “Helpdesk and Support” helping users use EOSC Federation services effectively.	7
LV-S-8	Interactive Notebooks integrated with storage and compute.	Available to authenticated users via eduGAIN and EOSC AAI.	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 for Synchrotron & Biophysics Research Researchers at Latvian Research Institutes often process terabytes of data from European Synchrotron facilities. This use case provides FileSender access via EOSC, using high-speed academic network to transfer large datasets securely between Latvia and foreign facilities, bypassing slow commercial cloud limits.	Value: Drastically reduces data transfer time for high-throughput experiments (e.g., Crystallography, Omics). Contribution: Demonstrates the value of the EOSC Connectivity layer for data-intensive science.	- 26 Research institutions in Latvia Especially data intensive RI: - LU CFI (Solid State Physics) - BMC (Biomedicine) - OSI (Organic Synthesis)	EOSC Federation	2026 Q4
LV-UC-2	Cross-Border Collaboration via Federated File Sync & Share (EFSS) Latvian researchers need secure shared workspaces with EU partners. This use case uses the EOSC Latvia Node's Nextcloud-based File Sync & Share service together with GÉANT eduTEAMS to manage virtual	Value: Simplifies collaboration; removes the need for multiple accounts; ensures data sovereignty and GDPR compliance. Contribution: Contributes to the EOSC "Collaboration" capability by federating national storage with EU identity.	- VPC (Service manager) - 26 Research institutions in Latvia	EOSC Federation	2027 Q4

	research groups, allowing project leaders to invite international colleagues using their home identities. Once authenticated, members gain access to shared project folders and resources in the Latvian Nextcloud instance without local account creation.				
LV-UC-3	Federated Discovery of Latvian Research Creation of a central metadata catalogue to integrate and expose Latvian research outputs to the EOSC Federation. The pilot phase aggregates DataverseLV, RSU Dataverse, and CLARIN-LV, establishing a scalable framework to progressively onboard all future national repositories.	Value: Eliminates fragmentation by providing a single, scalable registry for discovering Latvian research data across all disciplines. Contribution: Directly fulfils Federating Capability #2 by populating the EOSC Resource Graph with a sustainable, ever-growing stream of national metadata	- VPC (Coordinator) - RSU (RSU Dataverse) - IMCS UL (CLARIN-LV) - DataverseLV	EOSC Federation	2028 Q1
LV-UC-4	Access to Latvian EOSC Competence Centre The Latvian Data Stewards Network and EOSC Competence Centre will open selected support and training	Value: Addresses the "Skills Gap" in EOSC; provides human support where automated tools fail. Contribution: Contributes to the "Knowledge & Training"	- VPC (Coordination) - RSU, RTU, LU, LBTU	EOSC Federation	2028 Q1

	resources to the wider EOSC community, including training materials, guidelines, and access to 20+ data stewards across five institutions for RDM, FAIR and EOSC Latvia Node service questions.	layer of EOSC; shares a proven Data Stewardship model with other nodes.			

In scope - Project Outputs and Delivered Solutions

The primary scope of the EOSC Latvia Node is to establish a secure, interoperable, federated gateway that integrates Latvian research data and services into the EOSC Federation. The focus is on federating capabilities (connecting existing national assets) and knowledge transfer (Competence Centre). The Node will deliver:

- Federated data discovery: Deployment of a Central Metadata Registry aggregating metadata from DataverseLV (national), RSU Dataverse (institutional) and CLARIN-LV (language resources), and progressively other repositories. The registry will expose Latvian resources to the EOSC EU Node Resource Catalogue via OAI-PMH.
- Cross-border data transfer and collaboration: Deploying FileSender for high-speed, secure transfer of large datasets and a Nextcloud-based File Sync & Share service for international collaboration, both integrated with EOSC AAI via eduGAIN.
- Human Infrastructure: Operation of a National EOSC Competence Centre leveraging the Data Stewards Network across 5 major universities to provide training, videos, and support on FAIR data management and EOSC Latvia Node services to the wider EOSC community.
- Interoperability: Integration of the Latvian academic identity federation (LAIFE/eduGAIN) with the EOSC Federation AAI (MyAccessID) to enable seamless access for European researchers.

Stakeholder Support

The Node will support:

- National Research Performing Organizations (RPOs): 26+ Organisations in Latvia.
- European Researchers: Users from other EOSC Nodes requiring access to Latvian datasets or training materials.

Integration with EOSC Federation will use:

- AAI: OIDC/SAML integration via eduGAIN and MyAccessID.
- Metadata: OAI-PMH harvesting using EOSC profiles (DataCite, DCAT-AP/OpenAIRE).
- PID: DOIs (or equivalent PIDs) for deposited datasets to support FAIR principles.

Out of scope

To keep the build-up phase focused on federation and interoperability, the following are explicitly excluded:

- Creation of additional repositories; the Node will integrate and federate metadata from existing repositories.

- The development of entirely new software platforms or core services is out of scope; the EOSC Latvia Node will instead deploy, configure and federate existing mature solutions.

Limitations

- Initial language support will cover English and Latvian; translation of legacy dataset metadata into English remains the responsibility of data owners.
- Services will operate with defined quotas.

Dependencies

- EOSC EU Node: for central AAI proxy (MyAccessID) and EOSC Resource Catalogue/harvesting services.
- GÉANT and the Latvian academic network: for high-speed data transfer capabilities.
- Institutional data stewards and repository managers: for metadata quality and sustained onboarding at VPC and partner universities (LU, RTU, RSU, LBTU).

5. COMPLIANCE WITH TECHNICAL REQUIREMENTS

The EOSC Latvia Node fully confirms its agreement to comply with the EOSC Federation's mandatory technical specifications, including the EOSC Interoperability Framework and Rules of Participation. We commit to implementing all mandatory Federating Capabilities (AAI, Catalogue, Monitoring, Helpdesk) to ensure seamless technical integration with the EOSC EU Node and other Federation members.

Governance Structure

The EOSC Latvia Node is hosted by the Higher Education and Science IT Shared Services Centre (VPC), the nationally mandated organisation for EOSC and operator of the Latvian academic network, acting as the legal Node Host on behalf of the Ministry of Education and Science and signing the EOSC Federation MoU. The Node is led by a Coordinator, supported by an Operations Officer who manages the Node Operations Team at VPC and oversees day-to-day technical operations and EOSC integrations. A Cybersecurity Officer, Legal/procurement Officer and Communications Officer are appointed in line with the EOSC Federation Handbook, ensuring compliance with EOSC Rules of Participation, cybersecurity and legal requirements, and coherent communication with national stakeholders and EOSC governance bodies. Strategic oversight is provided by an Advisory Board representing the four major research universities (RTU, LU, RSU, LBTU), while long-term sustainability and investment capacity are secured through the ERDF-funded Project No. 1.1.1.6/1/25/I/001 (€16.74M, to November 2029) implemented by VPC.

Technical readiness

The Node builds on the upgraded high-speed academic network (LAT), with a planned 1.6 Tbit/s core and 100G/400G links to over 26 research institutions, meeting "hyper-connectivity" needs for data-intensive science. Compute and secure processing environments will be based on a production-grade cloud and TRE stack already proven within the EOSC ecosystem, ensuring that all services offered to EOSC users operate at TRL 7 or higher.

Integration in the EOSC Federated AAI

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

enabling cross-border SSO and controlled access to Latvian resources. Authentication will rely on eduGAIN-compatible solutions, including MyAccessID, and access to sensitive services will be restricted to Identity Providers meeting Assurance Level 2, with VPC supporting institutions to reach AL2 through guidance and training. GÉANT's eduTEAMS will be used to support virtual organisations for cross-node collaborations.

Exposure of Resources through the EOSC Catalogue

The Node will expose its resources to the EOSC Resource Catalogue via a National Metadata Aggregator, harvesting DataverseLV, RSU Dataverse, CLARIN-LV and other repositories. The aggregator will:

- 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 Latvia Node 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 based on eduGAIN and MyAccessID, providing federated access to Node Core and Node Exchange services.
- Helpdesk: an EOSC Latvia Node helpdesk at VPC, integrated with the EOSC Helpdesk via REST API, enabling bidirectional ticket routing for issues related to Latvian services.
- Monitoring: A unified monitoring system will continuously check the health, availability and reliability of Node services and publish standard metrics to the EOSC monitoring framework, 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 Latvia Node 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
Insufficient Funding Budget shortfall affecting	Risk is mitigated by secured ERDF Project No.	During the project

planned activities or sustainability.	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.	
Delays in Project Implementation Deviations from the planned timeline due to technical, organisational, or procurement delays.	Detailed work planning, monthly progress reviews, early risk detection, corrective action procedures, and formal change management for timeline adjustments.	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 GÉANT 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.	Security-by-design architecture, regular audits, incident response procedures, and dedicated IT security experts	During the project

7. CONTRIBUTIONS [DELIVERABLES (INCLUDING DOCUMENTATION)]

Deliverable ID	Deliverable Name	Responsible	Deadline
LV-DEL-1	Data Management and Transfer	VPC	2027 Q4
LV-DEL-2	EOSC Latvia Node Help desk	VPC	2027 Q3
LV-DEL-3	Central National Research Metadata Registry	VPC	2028 Q1
LV-DEL-5	National EOSC Competence Centre Platform	VPC	2028 Q1
LV-DEL-6	National Competence & Training Programme	VPC	2028 Q1

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 within Latvia, we will organize “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 (MyAccessID), 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 according to FAIR principles, how to practically implement Open Science workflows, and how to utilize EOSC Node services. This approach ensures sustainable, discipline-specific competence multiplication across the entire Latvian research ecosystem.

Capacity to Onboard Third-Party Resources EOSC Latvia Node is planned to be developed as an open "System of Systems" designed to aggregate resources beyond the founding consortium. We have allocated capacity to onboard up to 26 additional Latvian research institutions by 2029:
Standardized Onboarding: Third-party providers will receive a "Compliance Kit" (API guides, metadata templates, OAI-PMH configs) and access to a Test Environment to validate interoperability before production onboarding.
Policy Support: We will provide legal templates (Access Policies, Rules of Participation) to reduce administrative barriers for smaller institutes.
Pilot Credits: We allocate 2.5% of resources to "pilot research teams" to demonstrate early value and incentivize participation.

Using lessons from the current wave of Nodes EOSC Latvia Node embeds community engagement as a core activity, including training, consultations, usability feedback and targeted communication with its designated communities. Building on experience from the first-wave Nodes and the EOSC EU Node blueprint, we focus on three elements: continuous engagement through the Competence Centre and Technology Days, clear onboarding processes and documentation (Compliance Kit, pilot testing), and inclusive governance structures involving all major universities in steering Node priorities.

9. TIMING AND MILESTONES

ID	Milestone Description	Target Delivery Date

LV-MS-1	Highspeed connectivity between EOSC ecosystem elements (Establishment of the secure National Research & Academic Data Network 2.0)	2026 Q4
LV-MS-2	Service Deployment: Large File Transfer (FileSender) (Launch of FileSender service with EOSC AAI integration. User documentation published.)	2027 Q4
LV-MS-3	Service Deployment: Unified Metadata Registry (Operational aggregation of DataverseLV and partner repositories; exposure to EOSC EU Node Catalogue.)	2028 Q1
LV-MS-4	Competence Centre Establishment & Material Production (Formal launch of the National EOSC Competence Centre structure. Completion of the first batch of training materials (video tutorials, guidelines) for researchers and data stewards.)	2028 Q1

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 Latvia Node, each specialising in their respective field to ensure the successful creation of the Node.

Role	Name	Email
Coordinator	Inese Jaudzema	inese.jaudzema@vpc.lv
Operations Officer	1. Ilja Afanasjevs 2. Kristaps Oškalns	ilja.afanasjevs@vpc.lv kristaps.oskalns@vpc.lv
Cybersecurity Officer	Sarmīte Daņilova	sarmite.danilova@vpc.lv
Legal/procurement Officer	Sandra Jurago	sandra.jurago@vpc.lv
Communications Officer	Shelby Little	shelby.little@vpc.lv