EGI Foundation

openRDM.eu

Operational Level Agreement

Service Provider	EGI Foundation
Component Provider	EnhanceR
First day of service delivery	1st January 2021
Last day of service delivery	30th June 2023
Status	Final
Agreement finalization date	9th July 2021
Agreement Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v0.1	22/01/2021	First draft of the OLA, covering EGI ACE from Jan 2021 to June 2023	Alessandro Paolini
v1.0	27/05/2021, 09/07/2021	Review, aligned with existing ETHz SLA	Sergio Maffioletti, Alessandro Paolini, Andrea Manzi

TERMINOLOGY

The EGI glossary of terms is available at: http://go.egi.eu/glossary

For the purpose of this Agreement, the following terms and definitions apply. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Contents

The present Operational Level Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **ETH Zurich (the Component Provider)** to define the provision and support of the provided services as described hereafter. Representatives and contact information are defined in Section 6.

This Agreement is valid from **01/01/2021** to **30/06/2023**.

The Agreement was discussed and approved by EGI Foundation and the Component Provider **[date]**.

The Component Provider(s) is (are) bound by the terms and conditions of the EGI Default Operational Level Agreement[1] supplemented by the terms and conditions of this specific Agreement:

1 The Services

The Services are defined by the following properties:

Technical	The ***openRDM.eu*** service is based around the ARDM platform openBIS (https://openbis.ch/), developed for the last 12 years by the Scientific IT Services of Informatikdienste (ID SIS) at ETH Zurich. Active research data management (ARDM) is the process of organising data during an ongoing research project (data annotation, storage and backup). openBIS is a server-client application: the remote server hosts the database and storage backends which are accessed by the users from their local machines via a web browser. **openBIS** combines a data management platform with a digital lab notebook and a sample and protocol management system. It enables scientists to meet the ever-increasing requirements from funding agencies, journals, and academic institutions to publish data according to the **FAIR** data principles – according to which data should be Findable, Accessible, Interoperable and Reusable. The system is available in a version specific for life sciences and in a generic version, customizable for other scientific disciplines. openRDM.eu service consists of the following service components: ● Installation and configuration of openBIS server on cloud infrastructure ○ Including provisioning of cloud resources and their configuration ● Point-in-time recovery/backup of the PostgreSQL database up to 1 month.

[1] https://documents.egi.eu/document/2752

	Customer data backup includes: - a nightly volume snapshot that will be kept for 7 days; - daily copy of the openBIS data volume, including the PostgreSQL database, to a geo- redundant storage, in order to minimize risk of data loss. ● Regular upgrades of openBIS. ● Allocation of 100 GB of storage space. Storage can be extended at additional costs upon request. ● User support including data model needed to be able to import data into openBIS & training for the use of openBIS as data management tool. The service addresses two different customer segments. Firstly, researchers in Europe working in experimental and computational scientific fields, that require a day-to-day platform to manage their data. Secondly, IT departments that support these researchers. Besides, the service allows scientists to organize their experiments in a structured way, store the raw data and track subsequent data processing and analysis. Each scientist has a personal space in the ELN to organize projects and experiments. Furthermore, the service makes it possible to easily provide access to colleagues and external collaborators. Finally, through training the service increases awareness of research data management issues in the academic community. The customer has the possibility to test openBIS for 3 months. If the customer does not intend to continue using the service they need to notify ID SIS at openrdm.eu@id.ethz.ch within 3 months after the service has been provisioned. The service is currently deployed as a Swiss national service running on the SwitchEngines cloud infrastructure (based on OpenStack); Regular deployments are installed directly on the OS with the command-line installer. Authentication supports SWITCHaai infrastructure and the integration with EGI Check-in will be implemented during the EGI-ACE project. The service will be provided as managed instances running on the EOSC infrastructure. The EGI-ACE project will offer the service to its end-user base. These instances will include support for monitoring via the EGI Monitoring service and provide accounting records as specified by the EGI Accounting service.

	In addition to the managed instances, we will also offer support and consulting for on-premise deployment of the openRDM platform. ETH Zurich has a defined service target of 99.0% availability of the openBIS service during support hours (Monday to Friday, 09:00 – 16:00, except for public holidays in Zurich), excluding notified business interruptions (maintenance windows), errors or malfunctions of software due to user misconduct. The service provider will carry out the services to the best of their knowledge, exercising due care and taking into account the current state-of-the-art. The risk of data loss is minimized by implementation of redundant storage and geo-redundant backup. However, it is not possible to completely exclude the possibility of data loss.
Coordination	This activity is responsible for the coordination of the service maintenance activities with the EGI operations team and other relevant technology providers: ● EGI Cloud infrastructure ● EGI Check-in for authentication ● Storage (could be the same cloud infrastructure provider)
Operation	● Daily running of service instances (community dedicated instances upon request). ○ Maintenance and upgrade of the different openRDM.eu instances. ● Configuration and management of backup for datasets ● Database backups ● Incident handling ● Failover procedure to overcome or mitigate unexpected downtime of the service. ● Implementing all the measures for mitigating the risks listed in the Availability and Continuity Plan for the openRDM.eu service[2] ● Ensuring that best practices and processes are adhered to at any time.
Maintenance	This activity includes: ● Update and upgrade of the virtual instances hosting the different openRDM.eu services ● Update of the openBIS software stack ● Maintenance of monitoring probes to test the functionality of the service.

[2] https://wiki.egi.eu/wiki/Services_Availability_Continuity_Plans (to be created)

	• Documentation.

2 Service hours and exceptions

As defined in the EGI Default Operational Level Agreement.

IT services according to the service catalogue are in general delivered during 24 hours per day, 7 days per week (i.e. 365 days or 8,760 hours), to seamlessly support business operations. Planned and announced interruptions may reduce the effective operating time of a service.

The following exceptions apply:

- Planned maintenance windows or service interruptions ("scheduled downtimes"[3]) will be notified via email through the Broadcast Tool[4] in a timely manner:
  - 2-6 weeks in advance for maintenance during service hours,
  - 1 week in advance for maintenance outside of service hours.
- Unplanned maintenance windows are announced as early as possible ("best effort").
- Human services are provided during support hours.

3 Support

As defined in the EGI Default Operational Level Agreement.

Support is provided via EGI Service Desk[5] Support Unit: openRDM.eu

Access requires a valid X.509 or the login via an EGI Check-in account[6].

Support is available between:

- Monday and Friday
  9:00 and 16:00 CET/CEST time except for public holidays in the city of Zurich (see https://awa.zh.ch/internet/volkswirtschaftsdirektion/awa/de/arbeitsbedingungen/infos/feiertage.html). This excludes public holidays at the same time in all organizations providing the service.

Documentation and webinars for openBIS are available at https://openbis.ch/ .

Customer support is limited to a maximum of 5 working days in the first year of the service and 2 working days in the following years.

[3] https://wiki.egi.eu/wiki/GOCDB/Input_System_User_Documentation#Downtimes
[4] https://operations-portal.egi.eu/broadcast
[5] http://helpdesk.egi.eu/
[6] https://docs.egi.eu/providers/check-in/

3.1 Incident handling

As defined in the EGI Default Operational Level Agreement.

Incidents will be handled according to the Quality of Support level that is estimated according to the impact of the outage or service quality degradation.

The Quality of Support levels are defined as follows:

Medium level

In case of problems, our specialists are available Monday to Friday from 09:00-16:00.

The maximum response time for an incident during office hours is 1 working day. "Response Time" is defined as assigning a support engineer or contact with the user. The maximum "Time to Repair" is not and cannot be predefined.

Response time is provided as a service level target.

3.2 Service requests

As defined in the EGI Default Operational Level Agreement.

In addition to resolving incidents, standard service requests (e.g. change requests, information requests, documentation) will be fulfilled through the defined support channels in the same way as incidents. Service requests are classified as "Less urgent".

4 Service level targets

The service is available 7 x 24.

According to the ETHz rules for "white" services, the service hours are 09:00–16:00 Monday-Friday except holidays.

Outside of these hours, the service is provided on a "best effort" basis.

The target availability during service hours (excluding planned and unplanned security maintenance) is 99.0%.

Monthly Availability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month.
- Minimum during service hours (excluding planned and unplanned security maintenance), as a percentage per month: 99%

Monthly Reliability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods.
- Minimum during service hours (excluding planned and unplanned security maintenance), as a percentage per month: 99%

Quality of Support level

- Medium (Section 3)

5 Limitations and constraints

As defined in the EGI Default Operational Level Agreement.

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in the following language: English
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure. A party shall not be liable for any failure or delay in the performance of this Agreement for the period that such failure or delay is due to causes beyond its reasonable control. Means any
    - fire, flood, earthquake or natural phenomena,
    - war, embargo, riot, civil disorder, rebellion, revolution

which is beyond the Provider's control, or any other causes beyond the Provider's control.

6 Communication, reporting and escalation

6.1 General communication

The following contacts will be generally used for communications related to the service in the scope of this Agreement.

Service Provider contact	Alessandro Paolini operations@egi.eu EGI Foundation Operations officer
Component Provider contact	1. Sergio Maffioletti sergio.maffioletti@id.ethz.ch

	[Head Research IT Platforms] 2. Priyasma Bhoumik priyasma.bhoumik@id.ethz.ch [RDM Expert]
Service Support contact	See Section 3

6.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the service, the following reports will be provided:

Report title	Contents	Frequency	Produced by	Delivery
Service Performance Report	The document provides an overall assessment of service performance (per month) and OLA target performance achieved during reporting period	10 months (first report covering the period Jan – Oct 2021)	Component Provider	Survey form prepared by EGI Foundation

All reports shall follow predefined templates[7].

6.3 Violations

As defined in the EGI Default Operational Level Agreement.

The Component Provider commits to inform the Service Provider, if this Agreement is violated or violation is anticipated. The following rules are agreed for communication in the event of violation:

- In case of any violations of the Services targets, the Component Provider will provide justifications and a plan for Services enhancement to the Service Provider. The Component Provider will produce a status report and a Service enhancement plan for the improvement of the Services within one month from the date of the first notification.
- The Service Provider will notify the supporting Resource Centres in case of suspected violation via the EGI Service Desk. The case will be analysed to identify the cause and verify the violation.

[7] https://documents.egi.eu/document/2881

6.4 Escalation and complaints

For escalation and complaints, the Component Provider contact point shall be used, and the following rules apply.

- In case of repeated violation of the Services targets for **two consecutive months** or **four months over a period of 12 months**, a review of the Agreement and of the Services enhancement plan will take place involving the parties of the Agreement.
- Complaints or concerns about the Services provided should be directed to the Component Provider contact who will promptly address these concerns. Should the Service Provider still feel dissatisfied, about either the result of the response or the behaviour of the Component Provider, EGI Foundation Director director@egi.eu should be informed.

7 Information Security and data protection

As defined in the EGI Default Operational Level Agreement.

The following rules for Information Security and data protection should be enforced when they are applicable:

- The Component Provider agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident.
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements must be signed between EGI Foundation (the Data Controller) and Component Provider (the Data Processor).
- The Component Provider must comply with the EGI Policy on the Processing of Personal Data[8] and provide a Privacy Notice. This privacy Notice must be agreed with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[9].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policies[10].
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[11] in its most current version, which will be made available to the Component Provider by EGI Foundation upon request.

[8] https://documents.egi.eu/public/ShowDocument?docid=2732
[9] https://aarc-project.eu/policies/policy-development-kit/
[10] https://documents.egi.eu/public/ShowDocument?docid=3600
[11] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

- The Component Provider must meet all requirements of any relevant EGI policies or procedures[12] and also must be compliant with the relevant national legislation. Regarding EGI requirements, please refer to the following reference documentation:
    - EGI-doc-3015: e-Infrastructure Security Policy
    - EGI-doc-3601: Service Operations Security Policy
    - EGI-doc-2732: Policy on the Processing of Personal Data
    - EGI-doc-3600: Acceptable Use Policy and Conditions of Use
    - EGI-doc-2934: Security Traceability and Logging Policy
    - EGI-doc-2935: Security Incident Response Policy
    - EGI-doc-710: Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Component Provider

Additional responsibilities of the Component Provider are as follows:

- Adhere to all applicable operational and security policies and procedures[13] and to other policy documents referenced therein.
- Use communication channel defined in this agreement.
- Attend OMB[14] and other operations meeting when needed.
- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.
- Service with associated roles is registered in GOC DB[15] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[16].
- Changes in the system must be rolled in production in a controlled way in order to avoid service disruption.

8.1.1 Software compliance

Unless explicitly agreed, software being used and developed to provide the service should:

- Be licensed under an open source and permissive license (like MIT, BSD, Apache 2.0,...).
- The license should provide unlimited access rights to the EGI community.

[12] https://www.egi.eu/about/policy/policies_procedures.html

[13] https://www.egi.eu/about/policy/policies_procedures.html

[14] https://wiki.egi.eu/wiki/OMB

[15] http://goc.egi.eu/

[16] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

- Have source code publicly available via a public source code repository (if needed a mirror can be put in place under the EGI organisation in GitHub[17].) All releases should be appropriately tagged.
- Adopt best practices:
    - Defining and enforcing code style guidelines.
    - Using a Versioning schema.
    - Using a Configuration Management frameworks such as Ansible.
    - Taking security aspects into consideration at every point in time.
    - Having automated testing in place.
    - Using code reviewing.
    - Treating documentation as code.
    - Documentation should be available for Developers, administrators and end users.

8.1.2 IT Service Management compliance

- Key staff who deliver services should have foundation or basic level ITSM training and certification.
    - ITSM training and certification could include FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services.
- Component Providers should have clear interfaces with the EGI SMS processes and provide the required information.
- Component Providers should commit to improving their management system used to support the services they provide.

8.2 Of the Service Provider

The responsibilities of the Service Provider are:

- Raise any issues deemed necessary to the attention of the Component Provider;
- Collect requirements from the Resource infrastructure Providers;
- Support coordination with other EGI services
- Provide monitoring to measure fulfilment of agreed service level targets.

9 Review, extensions, and termination

There will be reviews of the service performance against service level targets and of this Agreement at planned intervals with the Service Provider according to the following rules:

- Technical content of the agreement and targets will be reviewed on a yearly basis

[17] https://github.com/EGI-Foundation

- EGI Foundation shall be entitled to conduct audits or mandate external auditors to conduct audits of suppliers and federation members. These will aim at evaluating the effective provision of the agreed service or service component and execution of activities related to providing and managing the service prior to the commencement of this agreement and then on a regular basis. EGI Foundation will announce audits at least one month in advance. The provider / federation member shall support EGI Foundation and all auditors acting on behalf of EGI Foundation to the best of their ability in carrying out the audits. The provider / federation member is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the provider / federation member will not be reimbursed.

The service is offered on a yearly basis to customers and is automatically renewed for one more year if not explicitly terminated. The customer must notify ETH Zurich, **ID SIS** in writing of the intention to discontinue the service with a notice period of 3 months before the end of the agreement of the current year.

Addresses of ETH Zurich, ID SIS are:

Scientific IT Services
ETH Zurich
Binzmühlestrasse 130,
CH-8092 Zürich
E-Mail: openrdm.eu@id.ethz.ch

When the service is discontinued by the customer, all data will be deleted. The service provider will advise customers of options for exporting their data from openBIS.

In case of termination of the service by the service provider, ETH Zurich will notify customers one year in advance. The service provider will provide all data stored in openBIS to the respective customers for download in a structured form.

10 Intellectual property rights

10.1 All preexisting intellectual property rights (rights to intangible property and related rights) shall remain with the respective pre-possessing party of this OLA. No preexisting intellectual property rights shall be transferred from one party to another by this OLA or by offering or using of the service described herein. Personal rights to intangible property remain reserved, provided they are not transferable by law.

10.2 All Copyrights of the software and the source code belong to ETH Zurich.