EGI VO

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Component Provider	**IFCA-LCG2**
Customer	DEEP Hybrid DataCloud consortium/deep-hybrid-datacloud.eu
First day of service delivery	01/01/2021
Last day of service delivery	30/06/2023
Status	FINAL
Agreement signature date	24/05/2021
SLA and OLA Link	https://documents.egi.eu/document/3747
Template Version	v2.13

DOCUMENT LOG

Issue	Date	Comment	Author
FINAL	24/05/2021	First version agreed with the Component Provider	Enol Fernández Giuseppe La Rocca
v0.2	13/01/2022	Updated OLA template (v2.13)	Giuseppe La Rocca

TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/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 **IFCA-LCG2 (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.

The DEEP Training Facility[1] is a distributed training facility for Machine Learning, Artificial Intelligence and Deep Learning models.

The DEEP Training Facility provides tools for building training, testing and training Machine Learning, Artificial Intelligence and Deep Learning models over distributed e-Infrastructures.

Models can be built from scratch or form existing and pre-trained models (transfer learning or model reuse). Ready to use models are available for transfer learning or reuse.

Features:

- **Transparent training over distributed e-Infrastructures with GPU access.**
- **Docker based for model portability and reusability.**
- **Easy model integration with standards-based REST APIs.**
- **CLI and web user interface to interact with the system.**
- **OpenID Connect based identity.**

The Customer is a DEEP Hybrid DataCloud consortium represented by **IFCA - CSIC**.

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

Once approved, **this Agreement is automatically renewed**, as long as the Component Provider does not express a decision to terminate the Agreement at least a month before the end date of the Agreement.

The Agreement was discussed and approved by the EGI Foundation and the Component Provider on **24/05/2021**.

The Agreement extends the Resource Centre OLA [1] with the following information:

1 The Services

Possible allocation types:

- **Pledged** - Resources are exclusively reserved to the Community.
- **Opportunistic** - Resources are not exclusively allocated, but subject to local availability.
- **Time allocation** - Resources are available for a fixed time period.

Possible payment mode offer:

- **Sponsored** - Model where the Customer uses services that are funded, or co-funded by the European Commission or government grants.

---

[1] https://marketplace.eosc-portal.eu/services/deepaas-training-facility

- **Pay-for-use** - Model where the Customer directly pays for the service used.

The Services are defined by the following properties:

Cloud Compute (category: Compute)

Description: https://www.egi.eu/services/cloud-compute/

- Resource Centre: **IFCA-LCG2 (Country: Spain)**
    - Cloud Compute
        - Number of virtual CPU cores: 500
        - Total memory (GB): 1000
        - Disk (GB):
        - Public IP addresses: 10
        - Payment mode offer: Sponsored
        - Other technical requirements: n/a
        - Duration: 01/01/2021 - 30/06/2023
    - Allocation type: Opportunistic
    - Provider AUP link:
    - Supported VOs: deep-hybrid-datacloud.eu
    - VO ID card: https://operations-portal.egi.eu/vo/view/voname/deep-hybrid-datacloud.eu
    - VO-wide list:
      https://vmcaster.appdb.egi.eu/store/vo/deep-hybrid-datacloud.eu/image.list
    - GOCDB endpoints urls: api.cloud.ifca.es (org.openstack.nova)

Online Storage (category: Storage)

Description: https://www.egi.eu/services/online-storage/

- Resource Centre: **IFCA-LCG2 (Country: Spain)**
    - Online Storage
        - Guaranteed block storage capacity [TB]: 1
        - Opportunistic storage capacity [TB]:
        - Standard interfaces supported[2]:
        - Storage technology[3]:
        - Other technical requirements:
        - Duration: 01/01/2021 - 30/06/2023
        - Payment mode offer: Sponsored
    - Allocation type: Opportunistic
    - Provider AUP link:
    - Supported VOs: deep-hybrid-datacloud.eu

---

[2] CDMI, POSIX, SWIFT, etc.
[3] DPM, dCache, STORM, etc.

- o   VO ID card: https://operations-portal.egi.eu/vo/view/voname/deep-hybrid-datacloud.eu
- o   GOCDB endpoints urls: N/A

2   Service hours and exceptions

As defined in Resource Centre OLA [1].

3   Support

As defined in Resource Centre OLA [1].

3.1   Incident handling

As defined in Resource Centre OLA [1].

3.2   Service requests

As defined in Resource Centre OLA [1].

4   Service level targets

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 (as a percentage per month): 95%

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 (as a percentage per month): 95%

Quality of Support level

- •   Medium (Section 3)

5   Limitations and constraints

As defined in Resource Centre OLA [1] and:

- •   Availability and Reliability calculations are based on the Service Monitoring operational results.

- Failures in VO monitoring are not considered as the Agreement violations.

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.

EGI Foundation contact	Giuseppe La Rocca
	sla@mailman.egi.eu
	SLA Coordinator at EGI Foundation
EGI Foundation technical contact	Matthew Viljoen
	operations@egi.eu
	Operations Manager at EGI Foundation
Component Provider contact	Alvaro Lopez
	aloga@ifca.unican.es
	Systems Manager
Component Provider technical contact	cloud.admin@ifca.unican.es
	Technical support contact
Service Support contact	See Section 3

6.2 Regular reporting

As defined in Resource Centre OLA [1].

6.3 Violations

The Component Provider commits to inform the EGI Foundation, if the Agreement is violated or violation is anticipated.

The following rules are agreed for communication at the event of the violation:

- In case of violations of the Services targets for **four months (within reporting period)** or **two consecutive months**, the Component Provider will provide justifications to EGI Foundation.
- In case of service target violation, the Component Provider must provide justifications and a plan for service enhancement **within 10 working days** from the date of the notification to/from the EGI Foundation.
  - In case of no or unsatisfactory justification and plan for improvement, EGI Foundation reserves the right to replace the Component Provider.

- EGI Foundation will notify the supporting Component Provider in case of suspected violation via the EGI Service Desk (Section 3). The case will be analysed to identify the cause and verify the violation.

6.4 Escalation and complaints

For escalation and complaints (a customer complaint is a customer's expression of dissatisfaction with an EGI service, either orally or in writing), EGI Foundation contact (Section 6.1) point shall be used, and the following rules apply.

- In case of repeated violation of the Services targets for **four months (within reporting period)** or **two consecutive months**, a review of the Agreement will take place involving the parties of the Agreement.
- Customer complaints or concerns about the Service(s) provided directed to the EGI Foundation contact will be shared with corresponding Component Providers.

7 Information security and data protection

As defined by the EGI Default Operational Level Agreement[4].

The following rules for Information Security and data protection must be enforced by the Component Provider:

- Make every effort to maximise the security level of users' data and minimise possible harm in the event of an incident. Incidents must be immediately reported to the EGI Computer Security Incident Response Team (CSIRT) according to the SEC01 procedure[5].
- For the processing of access data (ie. data related to authentication going through Check-in):
  - The roles according to GDPR are the following:
    - The Customer's Home Organisation holds the role of independent Data Controller.
    - EGI Foundation (the Service Provider) holds the role of independent Data Controller.
    - The Component Provider holds the role of independent Data Controller.
  - In this context there is no need for having any particular agreement in place.
- In the case the Customer, as a Data Controller, is processing any personal data (research data, personal data of their users or visitors) on the provided resources, EGI Foundation holds the role of Data Processor and the Component Provider the role of sub-processor. In that situation, when the Data Controller requests having a DPA signed with EGI Foundation as a processor, an additional subcontractor agreement has to be signed between EGI Foundation and the Component Provider as sub-processor.

---

[4] https://documents.egi.eu/document/2752
[5] https://go.egi.eu/sec01

- The Component Provider must comply with the EGI Policy on the Processing of Personal Data [6] and provide a Privacy Policy. This Privacy Policy can be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[7].
- The Component Provider must enforce the EGI Acceptable Use Policy and Conditions of Use.
- The Component Provider must comply with all principles set out by the GÉANT Data Protection Code of Conduct[8] (v1.0).
- Security incidents affecting the services described in Section 1 must be reported to abuse@egi.eu within 4 hours after their discovery and handled according to SEC01: EGI CSIRT Security Incident Handling Procedure.
- The Component Provider must meet all requirements of any relevant EGI policies or procedures[9] 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

8 Responsibilities

8.1 Of the Component Provider

As defined in Resource Centre OLA [1].

In addition:

- The Component Provider is responsible for monitoring of the usage and taking appropriate action to avoid overuse of resources defined in this agreement. EGI Foundation is not responsible for any costs incurred by over usage of what was otherwise defined in this agreement.

- The Component Provider shall not terminate the virtual machines without agreement with EGI Foundation.
  - Notification of resource termination shall be sent to the EGI Foundation 15 calendar days before.

---

[6] https://documents.egi.eu/document/2732
[7] https://aarc-project.eu/policies/policy-development-kit/
[8] https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers
[9] https://www.egi.eu/about/policy/policies_procedures.html

8.2 Of EGI Foundation

As defined in Resource Centre OLA [1] and:

- • Support coordination with other Component Providers;
- • Support coordination and conflict resolution with the Customer;
- • Support the Customer with data movement in case of OLA termination.

8.3 Of the Customer

- ● All responsibilities of the Customer are listed in relevant VO SLA.

9 Review, extensions and termination

As defined in Resource Centre OLA [1].

10 References

	Title	URL
[1]	Resource Centre Operational Level Agreement	https://documents.egi.eu/document/31