EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: Processing of personal data within the EOSC EU Node

Data Controller: European Commission, **Directorate-General** for Communications Networks, Content and Technology (also called **Connect**), CNECT.C.1 (hereafter "CNECT.C.1")

Processors:

Athena Research and Innovation Centre in Information Communication and Knowledge Technologies (Athena RC), Artemidos 6 & Epidavrou, 151 25 Maroussi, Athens, Greece (hereinafter "Athena RC");

Stichting EGI Foundation, Science Park 140, 1098XG Amsterdam, the Netherlands

NETCOMPANY-INTRASOFT S.A., 2B, Rue Nicolas Bové, Luxembourg, L-1253 Luxembourg

OpenAIRE AMKE, 6 Artemidos & Epidavrou, 151 25 Maroussi, Greece

Instytut Chemii Bioorganicznej Polskiej Akademii NAUK – Poznań Supercomputing and Networking Center Institute of Polish Academy of Sciences (PSNC), Noskowskiego 12/14, 61-704 Poznań, Poland (hereinafter "PSNC")

Record reference: DPR-EC-26549

Table of Contents

1. Introduction

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation "*Processing of personal data within the EOSC EU Node*" undertaken by CNECT.C.1 is presented below.

2. Why and how do we process your personal data?

Purpose of the processing operation: CNECT.C.1 collects and uses your personal information to provision the "EOSC EU Node" services.

The European Commission provides and maintains the EOSC EU Node that is a digital platform to enhance public access to information about research data, tools and services promoting the European Union's Policy on Open Science and European Strategy for Data. The EOSC EU Node is the first node of the European Open Science Cloud (EOSC) Federation (that is the collective name of the interoperable EOSC nodes connected with each other – the Federation does not have any legal personality).The EOSC Federation is the web of FAIR (Findable, Accessible, Interoperable and Reusable) data and services provided by the nodes, all together acting as an enabler for promoting and mainstreaming open science policies and practices, primarily aimed at researchers across the European Union. The processing of the users' personal data is carried out for the purpose of providing, managing and operating the managed services of the EOSC EU Node digital platform. In particular:

• **Authenticate users**. Authenticate users in the EOSC EU Node by the Federated AAI (Authentication and Authorization Infrastructure) service of the node provided by *Athena Research* and hosted by its sub-contractors and underlying providers: *GRNET* in Athens, Greece and *Amazon Web Services (AWS)* in Frankfurt, Germany. The Federated AAI service of the EOSC EU Node does not allow users to directly register but utilises existing Identity Providers (IdPs) of the users. There are two sets of IdPs:

- the EU Login service of the European Commission (including the eIDAS option);
- the eduGAIN inter-federation service for the research and education community operated by *GEANT Association (sub-contractor of ATHENA RC)*.

While EU Login (including eIDAS) covers the citizen scientist and EC staff, the eduGAIN inter-federation covers academia and researchers as the target users of the platform. The Federated AAI simply retrieves user attributes from those IdPs automatically.

The following personal data is requested by the Federated AAI services from the IdPs:

- First and last name
- Email address
- Username

- User identifier
- Country
- Organization
- Scoped affiliation (for eduGAIN users)
- Domain name (for EU Login users including eIDAS)

• **Authorize users and enforce Access Policies**. Allow authenticated users to access EOSC EU Node services, and define, monitor and enforce specific quota/service limits (which are modelled and communicated as 'virtual credits' according to the EOSC EU Node's User Access Policy (UAP) document in force). Authorization and policy enforcement services are provided by *Athena RC.* A user is authorized to access an EOSC EU Node service based on automated Access Policy Group allocation. The allocation decision into access policy groups uses attributes retrieved from the user's IdP.

- Access policy group "A" allows view-only access to all EOSC EU Node services based on the successful authentication of the user via the Federated AAI service (i.e. no particular user attributes are used). User gets no virtual credits.
- Access policy group "A1" allows full access to application services of the EOSC EU Node based on user attributes listed below (scoped affiliation value must be "employee" or "staff" in eduGAIN and domain value must be "eu.europa.ec" in EU Login). User gets 100 virtual credits allocated to use services.
- Access policy group "B" allows full access to both application and infrastructure services of the EOSC EU Node based on user attributes listed below (scoped affiliation value must be "faculty" member in eduGAIN). User gets 500 virtual credits allocated to use services.

Users in access policy group "B" are also allowed to invite other authenticated users from any other policy groups to their virtual team. Virtual team members are allocated 1000 virtual credits to be shared among themselves when using the services. All team members get the same authorization level to services.

Requests for additional quota/service limits and virtual credits for EOSC EU Node services may be examined on a case-by-case basis, following a user request and depending on the available resources.

The following personal data is used for automated access policy decisions and enforcement:

- Username
- User identifier
- Country (EU Member States and Horizon Europe Affiliated Countries)
- Scoped affiliation (for eduGAIN users)
- Domain name (for EU Login users including eIDAS)
- Entitlements (policy group for accessing services)
- Group membership

• **Accounting for EOSC EU Node services**. Allocate resources, monitor virtual credit consumption and services utilization, revise access policies, revoke credits and access to services, release under-utilized resources, ban users based on the EOSC EU Node's Acceptable Usage Policy (AUP) and User Access Policy (UAP) documents in force. Virtual credits may be revoked from users in case of misuse of services and resources (e.g., less than 5% of CPU utilization for 30 consecutive days). Users may be banned if they violate the AUP terms. Accounting services are provided by *Athena RC.*

The following personal data is used by the Accounting service:

- First and last name
- Email address
- Username
- User identifier
- Entitlements (policy group for accessing services)
- Group membership
- User agent
- IP address
- Timestamps
- Resource consumption (credit balance and spending, orders, allocation, utilization)

• **Knowledge Graph (KG) of Research Products**. Provision a KG of Open Science research products (scientific publications, data, software, tools, training) and EOSC EU Node infrastructure and application services, to enable open and FAIR scholarly communication for authenticated users. The KG is created by harvesting and aggregating (i) existing open data sources (e.g., OpenAIRE, CORDIS) which contain author information as per scholarly communication practices, (ii) EOSC EU Node catalogues (e.g., training material, tools), and (iii) catalogues of similar open scholarly content from other EOSC Nodes (in the future). The KG handles information about user identities and favourite items of the authenticated users and passes that information to other services of the EOSC EU Node.. These services are provided by *OpenAIRE AMKE* and *Athena RC.*

The following personal data is used by the Knowledge Graph service:

- Username
- User identifier
- Resources created
- Resources targeted (viewed, accessed)
- Resources shared (downloaded, commented)

• **Application Workflow Management service**. Allow authenticated users to create their own configuration files and templates (e.g., configuration files needed e.g., to deploy a specific application in a selected infrastructure) published and shared via the KG and automatically used in the infrastructure services of the EOSC EU Node. Shared configuration files allow users to repeat experiments easily. This service is provided by *Stichting EGI Foundation.*

The following personal data is used by the Application Workflow Management service:

- Username
- User identifier
- IP address
- Group membership
- Resources created
- Resources targeted (viewed, accessed)
- Resources shared (downloaded, commented)

• **Personalized Recommendations**. Recommend to authenticated users who have turned on this feature (this feature is based on consent collected at first-time login) relevant Research Products of the Knowledge Graph based on their past search criteria and navigation history (e.g., recommend a scientific data set based on the user's search queries and viewed publications). This personal recommendation service is provided by *OpenAIRE AMKE* and their sub-contractors.

The following personal data is used by the Recommendation service:

- Username
- User identifier
- Resources created
- Resources targeted (viewed, accessed)
- Resources shared (downloaded, commented)
- Resource consumption (credit balance and spending, orders, allocation, utilization)
- Search history

• **Provision of Infrastructure and Application Services from the EOSC EU Node**. These include commoditized and research-focused infrastructure services (Virtual Machines, Container Platform Services and Bulk Data Transfer) and application services (Interactive Notebooks, File Sync & Share and Large File Transfer Service) offered for free at the point of use by the EOSC EU Node to its authenticated users. Access policy group “A1” allows access to application services, access policy group “B” allows access to both application and infrastructure services, in accordance with its User Access Policy and Acceptable Usage Policy documents in force. These infrastructure and application services are provided by *PSNC* and their sub-contractors.

The infrastructure and application services of the EOSC EU Node process the following personal data:

- First and last name
- Email address
- Username
- User identifier
- Entitlements (policy group for accessing services)
- Group membership
- User agent
- IP address
- Timestamps
- Resource consumption (credit balance and spending, orders, allocation, utilization)

• **Performance & Service Level Agreement (SLA) monitoring**. Monitor and fine-tune the performance, availability and scalability of the EOSC EU Node services (e.g., provisioning of resources, indexing, scaling of cloud resources) to ensure a high-quality user experience and within the target SLAs. This service includes processing of logs and logging history of the users and their IP addresses. These services are provided by *Stichting EGI Foundation.*

The following personal data is used by the monitoring service:

- Username
- User identifier
- Entitlements (policy group for accessing services)
- Group membership
- User agent
- IP address
- Timestamps
- Resource consumption (credit balance and spending, orders, allocation, utilization)

• **Helpdesk service.** Helpdesk provides support for authenticated users (all groups) regarding all technical and administrative aspects of the operation, maintenance and support of the EOSC EU Node. The first line helpdesk support is implemented as a web form where authenticated users can first contact the operators briefly describing their issue. The helpdesk operators then create a ticket in the Helpdesk system (implemented by the open-source software tool called Zammad) and inform the user via e-mail. The user can track the ticket in the Helpdesk system directly provided via the link in the e-mail. The first line support may pass forward the ticket to second and third line support helpdesks, operated by the particular service providers with deep technical knowledge. The first line helpdesk service is provided by *Stichting EGI Foundation* and their subcontractors.

The Helpdesk service of the EOSC EU Node process the following personal data:

- First and last name
- Email address
- Username
- User identifier
- Entitlements (policy group for accessing services)
- Group membership
- User agent
- IP address
- Timestamps
- Resource consumption (credit balance and spending, orders, allocation, utilization)
- Specific issue as described by the user.

3. <u>On what legal ground(s) do we process your personal data</u>

The use of the EOSC Node is the choice of each user: for this reason, the processing activities herein described and necessary for the delivery of the services which constitute the EU EOSC Node is based on consent. Consent is obtained by explicitly asking the user to agree to the personal data processing for the specific purpose of the EOSC EU Node services on the consent page (box to tick) presented to the user at first-time login. Consent for the use of the platform is collected as follows: "I consent to the processing of my personal data entailed by the use of the EU EOSC Node as described in the privacy statement" these actions are in full alignment with Articles 3 (15) and 7 of Regulation (EU) 2018/1725.

4. <u>Which personal data do we collect and further process</u>*?*

In order to carry out this processing operation CNECT.C.1 collects the following categories of personal data:

- First and last name
- Email address
- Username
- User identifier
- Scoped affiliation (for eduGAIN users)
- Domain name (for EU Login users)
- Organization
- Country (for eduGAIN and eIDAS users)
- Entitlements (policy group for accessing services)
- IP address (if it is not masked)
- User agent (client)
- Timestamps
- Resources created

- Resources targeted (viewed, accessed)
- Resources shared (downloaded, commented)
- Resource consumption (credit balance and spending, orders, allocation, utilization)
- Search history
- Group membership
- Specific issue as described by the user (to Helpdesk)

The provision of personal data is not mandatory. We obtain your personal data from your Identity Provider (IdP) when you login the EOSC EU Node.

5. How long do we keep your personal data?

CNECT.C.1 only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely a maximum of 5 years from your first successful login to the EOSC EU Node or until the user requests to delete the relevant personal data via Helpdesk, as specified in the relevant Record.

This administrative retention period of five years is based on the retention policy of European Commission documents and files (and the personal data contained in them), governed by the common Commission-level retention list for European Commission files SEC(2019)900. It is a regulatory document in the form of a retention schedule that establishes the retention periods for different types of European Commission files. That list has been notified to the European Data Protection Supervisor.

The administrative retention period is the period during which the Commission departments are required to keep a file depending on its usefulness for administrative purposes and the relevant statutory and legal obligations. This period begins to run from the time when the file is closed.

In accordance with the common Commission-level retention list, after the 'administrative retention period', files including the Knowledge Graph (and the personal data contained in them) can be transferred to the Historical Archives of the European Commission for historical purposes (for the processing operations concerning the Historical Archives, please see record of processing 'Management and long-term preservation of the European Commission's Archives', registered under reference number DPR-EC-00837).

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission or of its contractors. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679.]

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

- Within the EU organization
  - European Commission staff of the Commission service owning the EOSC EU Node and engaged in monitoring, managing, supervising, and auditing the external Contractors working on behalf of and under contractual agreement with the Commission for the managed service provision of the EOSC EU Node.
  - European Commission Staff of other Commission Services may have access on a "need to know" basis (e.g., policy monitoring/planning, cyber security).
- Outside the EU organization
  - Contractors working on behalf of and under contractual agreement with the Commission service owning the EOSC EU Node and engaged the managed service provision of the EOSC EU Node.

Please note that pursuant to Article 3(13) of Regulation (EU) 2018/1725 public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have consented to provide your personal data to CNECT.C.1 for the present processing operation. You can withdraw your consent at any time by notifying the Data Controller. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, CNECT-C1@ec.europa.eu

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-26549.