EOSC Portal AAI Privacy Policy

Version 1.0, August 1, 2018

This Privacy Policy explains how we, the EOSC Portal AAI service (“We”), treat data by which you can be personally identified (“Personal Data”) as a result of your registration for and use of the EOSC Portal infrastructure (“Infrastructure”).

To enable the Infrastructure to be safe and reliable for your use and to preserve your rights as a user we adhere to "The EGI Policy on the Processing of Personal Data" (“The Data Protection Policy”) available in the Appendix below. The Data Protection Policy should also be read with reference to other Infrastructure policies available at https://wiki.egi.eu/wiki/SPG:Documents.

What Personal Data do We process?

We collect and process the following Personal Data to identify you, thereby enabling us to grant you access to the services and resources provided by the Infrastructure:

- Data for User authentication
    - Identifiers unique to you as released by your authentication service
- Data for registration with the EGI CheckIn service and for collaboration management
    - Your name
    - Your Institute
    - Your e-mail address
- Data which may be used to grant you access to the services
    - Home Institute, Infrastructure and User Community specific information relating to your affiliations and roles

Purposes of Processing

We process your personal data solely to manage your access to the EOSC Portal AAI service and other Infrastructure services, including those provided by User Communities, all bound to the same Infrastructure policies.

Your personal data will be used solely for administrative, operational, monitoring, security and dispute resolution purposes.

Your usage of the Infrastructure will be monitored and records of this use, containing your Personal Data, will be stored and used only for the same purposes.

Stored where?

The records of your use of the Infrastructure are stored in secure databases in various locations at EGI Resource Centres and EGI Operations and Accounting centres, all of whom are bound by the obligations of this Privacy Policy and the Data Protection Policy.

Accessed by whom?

The records of your use may only be accessed by appropriately authorised individuals in EGI/NGI Operations, in the EGI CSIRT and NGI security teams and authorised resource managers in your User Community.

Retained for how long?

The records of your use of the service(s) will be deleted or anonymised after, at latest, 18 months.

Sharing of your Personal Data with others

Your Personal Data will be shared with other authorised Infrastructure participants via secured mechanisms, only for the purposes given above, and only as far as necessary to manage your access to the service(s), any only where the recipient has agreed to abide by this Privacy Policy and the Data Protection Policy.

The records of your use may be shared for security incident response purposes with other authorised participants in the academic and research distributed digital infrastructures via secured mechanisms, only for the same purposes and only as far as necessary to provide the incident response capability where doing so is likely to assist in the investigation of suspected misuse of Infrastructure resources.

Name and Contact details of Data Processor

The EGI.eu Operations Team. (email: operations@egi.eu)

Name and Contact details of the EOSC Portal AAI Service Data Protection Officer

You can contact our Data Protection Officer (Matthew Viljoen, EGI Operations, email: matthew.viljoen@egi.eu) to obtain a copy of your Personal Data, request that it is corrected in case of factual error or if you suspect that it has been misused. You can also request that we stop using your Personal Data but this will affect your access to the Infrastructure.

Appendix: "The EGI Policy on the Processing of Personal Data"

Introduction

The "EGI Policy on the Processing of Personal Data" (hereafter referred to in this Appendix as this "Policy" or the "Policy") ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains “personal data” as defined by the European Union (EU) [R1]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

Definitions

Infrastructure
: The bounded collection of universities, laboratories, institutions or similar entities, which adhere to a common set of policies [R2] and together offer data processing and data storage services to End Users.

Participant
: Any entity providing, managing, operating, supporting or coordinating one or more Infrastructure service(s).

Personal Data
: Any information relating to an identified or identifiable natural person [R1].

Processing (Processed)
: Any operation or set of operations, including collection and storage, which is performed upon Personal Data [R1].

End User
: An individual who by virtue of their membership of a recognised research community is authorized to use Infrastructure services.

Scope

This Policy covers Personal Data that is Processed as a prerequisite for or as a result of an End User’s use of Infrastructure services. Examples of such Personal Data include registration information, credential identifiers and usage, accounting, security and monitoring records. This Policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.

Policy

By their activity in the Infrastructure, Participants:

a. Declare that they have read, understood and will abide by the Principles of Personal Data Processing as set out below.
b. Declare their acknowledgment that failure to abide by these Principles may result in exclusion from the Infrastructure, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

Principles of Data Processing

i. The End User whose Personal Data is being Processed shall be treated fairly and in an open and transparent manner.
ii. Personal Data of End Users (hereinafter “Personal Data”) shall be Processed only for those administrative, operational, accounting, monitoring and security purposes that are necessary for the safe and reliable operation of Infrastructure services, without prejudice to the End Users’ rights under the relevant laws.
iii. Processing of Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed.
iv. Personal Data shall be accurate and, where necessary, kept up to date. Where Personal Data are found to be inaccurate or incomplete, having regard to the purposes for which they are Processed, they shall be rectified or purged.
v. Personal Data Processed for the purposes listed under paragraph ii above shall not be kept for longer than the period defined in a relevant Infrastructure service policy governing the type of Personal Data record being Processed (e.g. registration, monitoring or accounting) and by default shall be anonymised or purged after a period of 18 months.
vi. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. As a minimum, Infrastructure Participants shall:
    a. Restrict access to stored Personal Data under their control to appropriate authorised individuals;
    b. Transmit Personal Data by network or other means in a manner to prevent disclosure to unauthorised individuals;
    c. Not disclose Personal Data unless in accordance with these Principals of Personal Data Processing;
    d. Appoint at least one Data Protection Officer (DPO) with appropriate training and publish to the Infrastructure a single contact point for the DPO to which End Users or other Infrastructure Participants can report suspected breaches of this Policy;
    e. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred;
    f. Perform periodic audits of compliance to this Policy and make available the results of such audits to other Infrastructure Participants upon their request.
vii. Each Infrastructure service interface provided for the End User must provide, in a visible and accessible way, a Privacy Policy containing the following elements:

a. Name and contact details of the Participant Processing Personal Data;
b. Description of Personal Data being Processed;
c. Purpose or purposes of Processing of Personal Data;
d. Explanation of the rights of the End User to:
    i. Obtain a copy of their Personal Data being stored by the Participant without undue delay;
    ii. Request that any Personal Data relating to them which is shown to be incomplete or inaccurate be rectified;
    iii. Request that on compelling legitimate grounds Processing of their Personal Data should cease;
e. The contact details of the Participant's DPO to which the End User should direct requests in relation to their rights above;
f. Retention period of the Personal Data Processed;
g. Reference to this Policy.

viii. Personal Data may only be transferred to or otherwise shared with individuals or organisations where the recipient
    a. has agreed to be bound by this Policy and the set of common Infrastructure policies,
    or
    b. is part of a recognised Computer Incident Response Team framework and as part of an incident investigation to prevent active or suspected misuse of Infrastructure services,
    or
    c. presents an appropriately enforced legal request.

References

[R1]: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD)
http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046
[R2]: Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents