Science Mesh Privacy Policy

Status	**Draft**
Date	**14 february 2022**
DOI	**10.5281/zenodo.6089064**

Document log

Issue	Date	Description	Author
v. 0.1	28-01-2022	Initial version	Renato Furter, Ron Trompert
v. 0.2	02-02-2022	Distinction of end users and personnel introduced, text structure modified	David Antoš
v. 0.3	09-02-2022	Description of end user policies added	David Antoš
v. 0.4	14-02-2022	Received comments incorporated	Ron Trompert

Terminology

The Science Mesh glossary is available at: https://doi.org/10.5281/zenodo.5038662

For the purpose of this document, 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.

Table of Contents

Introduction

In this document describes the Science Mesh Privacy Policy. The policy has two distinct parts: one relating to Science Mesh end users, the other relating to administration of the Science Mesh as an infrastructure, affecting personnel of the infrastructure and its Sites.

Description of the Service

Science Mesh is an infrastructure of independent data storage Sites providing sync-and-share services also called Enterprise File Synchronisation and Sharing (EFSS) services. It is a loose federation allowing users of the Sites to share and transfer data among the Sites and to access applications running in the infrastructure without prior detailed knowledge of technical details like which systems their colleagues use and what are their user identities in them.

In order for the systems to share data, the Open Cloud Mesh protocol and CS3 API is used. The protocol and the API handle accessing and exchanging data, but they solve neither discovery of user identities nor establishing trust between EFSS systems that are necessary to make such a sharing practical for the administrators and the users.

Those two main layers are therefore added by the Science Mesh:

- the Science Mesh is an infrastructure with metadata describing its Sites and services (so that adding a site does not require configuring all other Sites in the infrastructure individually),
- handling user identities is quite hidden from the users who may use any standard way of textual communication such as e-mails or instant messaging to establish trust with their colleagues to share data with them, i.e. by sending user-friendly invitations.

The Science Mesh is an instance of such a federation.

End Users of the Science Mesh

When sharing resources such as folders, files, or application access, we need to distinguish two end users of EFSS: an originating user is the user with the resource to be shared who intends to invite a target user to access the resource. The originating user initiates the process by sending and invitation to target user's email address (or any other textual communication, but the principles are identical). Note that it is originating user's responsibility to posses target user's email address in a lawful manner, it is out of scope of the Science Mesh.

The target user receives the invitation with instructions to open a web service running at the originating site. The target user uses this service to select the target system out of a list of Sites in the Science Mesh, logs into the target system and thus reveals which user account in the target system should be associated with the email address. The user identity and his/her EFSS retrieved in this step is necessary to establish sharing of the resource. The target EFSS and the target user's identity on this service is the sole information that may be cached at Science Mesh Sites. The target user is free to choose not to proceed with the procedure at any point (e.g. to ignore the invitation). Suppose the relationship between target user's email address and user account in the target system gets established. Then it is used solely for the purpose of sharing the resource in question (based on legitimate interest to provide the requested service).

During the procedure, the target user is asked to consent to this relationship to be cached for the originating user: this is particularly useful as users tend to share more resources than one with each other. Should the target user consent to caching this trust relationship, then the relation of target user's email address and user account in the target system is stored in the originating system in an address book of the originating user. No other users of the originating site have access to this information. While users are encouraged to consent to caching (to make future operations easier for them), caching the information is not strictly necessary for the Science Mesh to operate and is therefore purely based on consent of the target user. The relationship is stored until

- originating User's account in the originating system is deleted and then discarded with it,
- or the originating site gets information that the relationship is no longer valid (e.g. attempting to share another resource and receiving error from the target site that the target account is no longer present),
- or the target user requests deletion of this information (based on the "right to be forgotten"). Users may request deletion of cached information in the Science Mesh or in a specific originating site; the point of contact for the target user to file such a request is target system's standard helpdesk.

Target user's information stored by originating sites is subject to particular originating Site's privacy policy. The privacy policy MUST have a clause handling deletion of cached information from the Science Mesh.

Site Administrators and Other Personnel

In order to establish an infrastructure, collecting information about Sites and their personnel is necessary. The rest of this policy deals with personal information of operators of Science Mesh Sites, administrative contacts, and other personnel taking part in Science Mesh operations. All of this staff is referred to as Site Representatives in the remainder of this policy.

Architecture of the Science Mesh

The Central Component of the Science Mesh infrastructure possesses a Central Database that holds personal information described in the following sections. This is the only place where personal data is stored that is needed for Science Mesh operations.

The Central Database is provided by (name of the site hosting the Central Database) on behalf of the Science Mesh. The Central Database is a central registry to record information about the topology of the Science Mesh infrastructure. This includes information describing operations and resource centres, network connection endpoint and downtimes of services, and the roles and contact information of related personnel.

(name of the site hosting the Central Database) complies with the requirements of the European General Data Protection Regulation with regard to the collection, storage, processing and disclosure of personal information and are committed to upholding the GDPR's core data protection principles.

A full notice of the position of (name of the site hosting the Central Database) with regards to Freedom of Information and the GDPR (EU) (2016/679) can be found at: (link).

If you have any questions or remarks, please contact us at: (helpdesk address)

Data controller	Fill in
Data protection officer	Fill in
Supervisory authority	Fill in
Jurisdiction	Fill in

Further details on how to raise concerns or report problems exercising your rights regarding your personal data can be found here: (link)

Personal data collected and its purposes

Registration

In order to be able to add or modify the metadata of a Site in the Central Database, at least one Site Representative needs to have an account first. This can be done by registering the following information:

- name of your Site
- first name and last name
- email address
- telephone number (optional)
- security contact

This data is necessary for account management purposes (e.g. to contact you to inform you of changes to the service or for security purposes), and for the reasons given in the paragraph below.

Information associated with your account

You may optionally request that the following information be associated with your account

- a Site and/or other administrative entity
- one or more roles you are authorised to hold (e.g. Site Administrator) at that entity.

This data is necessary to allow other authorised users, and/or automated services acting on their behalf, to recognise and contact you in a reliable manner.

Login

Each time you access the Central Database then your login name is collected. This data is necessary for security purposes to uniquely identify and authenticate you when creating and subsequently accessing your account.

Logs

Log records of your access to and actions on the Central Database are retained. These records contain

- your unique identifier (as in “Login” above)
- the network (IP) address from which you access the Central Database
- the time and date of access
- details of actions you perform.

This data is necessary to ensure that the Central Database service is reliable and secure, such as for assisting in the analysis of reported problems, contacting you if a problem is identified with your account and responding to security incidents.

1Parties to whom personal data is disclosed

Your personal data will be disclosed only to other *authorised* users of the Central Database and only for the reasons stated above. All *authorised* Central Database users, on registration for a Central Database account, have agreed to use personal data purely for the appropriate purposes described above.

Recipients of your personal data, as defined above, will not be located in a country outside of the European Economic Area or in a country without an adequate level of data protection pursuant to Article 45.1 of the GDPR or in an International Organisation.

2Access, rectify and delete personal data and object to its processing

For these issues, contact (helpdesk address).

3Data retention

Records of your use of the Central Database, collected for reasons of security (described in the section “Logs” above) will be deleted, at latest, 6 months after your last use of the service.

Other personal data can be deleted immediately or on request as described above.

4Data protection

Appropriate technical and organisational measures are taken against unauthorised disclosure or processing of personal data and against accidental loss or destruction of, or damage to, personal data. A prompt response to suspected breaches of this policy SHALL be undertaken and the appropriate action SHALL be taken.

Personal data MAY only be transferred to or otherwise shared with individuals or organisations where at least one of the requirements below apply for the recipient:

- The recipient is part of the Operational Team and has agreed to be bound by this policy.
- The recipient 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
- The recipient presents an appropriately enforced legal request

Personal data SHALL only be transferred in such a way as to prevent disclosure to unauthorised individuals.