eduroam Privacy Notices - Changes for Managed IdP

Description of the eduroam Service

eduroam (education roaming) is a secure, world-wide roaming access service developed for the international research and education community. eduroam allows any user from an eduroam participating site to get network access at any location that provides eduroam service.

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at his/her home institution (Identity Provider, IdP) using the institution's specific authentication method. The authorisation required to allow access to local network resources is carried out by the visited institution (Service Provider, SP).

Thus, the eduroam roaming consortium is comprised of many legal entities: (N)ROs, IdPs and SPs. (National) roaming operators ((N)RO) are entities that operate the eduroam service for a country or economy and coordinate the activity of IdPs and SPs in the respective territory.

GÉANT is the body which is responsible for the international coordination and interoperability of eduroam. As such GÉANT operates a number of services for the eduroam community, from the technical infrastructure at the European level to supporting services aimed for the world-wide community. Those services are maintained by eduroam Operations Team (OT). This privacy policy concerns part of the eduroam service that is operated and maintained by GÉANT including, but not limited to, the following services:

- **The European level authentication proxy infrastructure,**
- **The eduroam database,**
- **The eduroam Configuration Assistant Tool (CAT),**
- **The eduroam Managed IdP Service,**
- **The eduroam F-ticks traffic measurement,**
- **The portal with technical information about the service - monitor.eduroam.org,**
- **The eduroam wiki, and**
- **The eduroam website.**

eduroam was designed for minimal disclosure of end users' personal data following the requirement that user must be authenticated by his/her IdP. The design of the system provides and favours the end user anonymization, i.e., the possibility to hide the end user's identity from any third parties, including providers of eduroam network access (SPs). eduroam technical foundations have a built-in support for end user privacy throughout the authentication process. For all intermediate services, like routing of authentication requests and F-ticks (log format for distributed federations), the service is designed to know *nothing* about the actual identity of an end user, while still maintaining log traces which allow for resolving security incidents, debugging, monitoring and usage statistics.

To view the general Privacy Notice for GÉANT, please visit the GÉANT website.

Why We Process Personal Data

We process various data in order to provide a reliable and secure eduroam service and to ensure and improve the quality of the eduroam supporting service. The eduroam service is designed in a way that we don't need to know end user identity in order to provide the service. Partners within eduroam community can anonymise potential end user's private data. We give advice and guidance to the community that recommends the highest levels of anonymity of data in all deployments.

For the eduroam Managed IdP service which may be used by some home organisations to outsource technical part of the IdP function, we process personal data in order to provide the end users with the eduroam access credentials in the highest privacy preserving manner.

We also collect data related to NROs, IdPS and SPs to enable supporting services and improve incident response and user support. Access to the data collected in the eduroam database and other supporting services which is considered private is limited (via authentication mechanism based on eduGAIN) to responsible personnel of GÉANT and NROs.

What Personal Data We Process

As part of the eduroam service, we process the following data:

- When you roam and visit other countries, or as a user of the eduroam Managed IdP service, the European proxy servers will receive and log the following data: **your realm (denoting your institution and federation) and MAC addresses**. We can also receive **your username** if you have not chosen to anonymise this data (eduroam Managed IdP always uses opaque usernames). When you roam to another institution within your home country the European proxy servers don't receive any data because they are not included in that process. The service has a **legitimate interest** in processing this information.
- When you roam and visit other countries or other institutions within your federation we may also process for monitoring, measuring and reporting services, in addition to the data mentioned above, the data about **visited country, visited institution and authentication outcome**. The service has a **legitimate interest** in processing this information.
- As part of supporting activities we maintain several public web sites (e.g. web site of the Configuration Assistant Tool - CAT service https://cat.eduroam.org) of) where we collect normal web server logs, i.e. **timestamp of access, IP address which requested the page, the page being requested, the HTML result code**, etc. The data collected is for the purpose of troubleshooting and debugging potential problems of with eduroam web servers and therefore the service has a **legitimate interest** in processing this information.
- The eduroam Operational Team maintains a database where we collect data that may include **name**, **e-mail**, **phone number** of the NROs, IdPS and SPs contacts to enable supporting services and improve incident response and user support. The data is provided by the NROs based on the eduroam Policy Service Definition. eduroam strongly advises NROs to use the function contacts rather than the personal ones.
- To ensure proper functioning of the eduroam Configuration Assistant Tool (CAT) and of the eduroam Managed IdP service we collect the **identifiers** and **e-mail addresses of the NRO and IdP administrators** responsible for the configurations that will be used by the end users. The service has a **legitimate interest** in processing this information.

- The eduroam Managed IdP system also stores an **arbitrary identifier** for you (given by the IdP administrator), and maintains **pseudonyms of that identifier** for the actual eduroam access credentials. It also stores information about **successful authentications** linked to those pseudonyms. This processing is part of the contractual requirements for eduroam Managed IdP as part of service delivery.
- Your IdP administrator for eduroam Managed IdP may choose to send you an invitation link via **SMS** or **e-mail**. We will process this data in order to send you the invitation link but the data will not be stored.

Who Do We Share Data With?

Personal data gathered for website statistics is only shared within the GÉANT Association and the eduroam Operational Team for analysis and reporting.

The contact information collected in the eduroam database is used by the OT and NROs in order to resolve security incident and debug problems reported by the end users.

Personal data collected for the eduroam Managed IdP are available only to the IdP administrators.

All other personal data is held and processed only by the eduroam OT.

Personal Data Retention

Analytical data for website statistics is currently retained permanently.

All data related to roaming are kept for a period of six months, unless a different requirement is set by legislation in individual European countries.

Personal data stored as part of your credentials issued via eduroam Managed IdP are kept as long as you use those credentials for eduroam access, and until they are removed by the IdP administrators. SMS or e-mails processed in order to send you invitation links are not retained.

Security

We support the following processes to ensure the security of your data:

- Managing, limiting and controlling access to personal data;
- Resilience of processing systems and services;
- Your personal data is securely destroyed when no longer required;
- Regular testing of the effectiveness of measures implemented.

With these measures we intent to minimize the risk of disclosure of your personal data.

Your Rights

You have the following rights regarding your personal data:

- You have the right to request access to your data;
- You have the right to ask us to rectify information;
- You have the right to ask us to erase your personal information;
- You have the right to object to your data being processed.

We keep this Privacy Notice under regular review. This Policy was last updated in November 2018.

In order to exercise those rights please contact: GDPR@GEANT.ORG

You also have the right to inquire what personal data we hold about you, and to present a complain to the Supervisory Authority (Autoriteit Persoonsgegevens at https://autoriteitpersoonsgegevens.nl) about our personal data processing activities if you feel your personal data is not being managed as described here.

Please feel free to contact us for any further questions, through this email address: GDPR@GEANT.ORG

Contact Information

Data Controller and Contact	**Data Protection Officer** GÉANT Association Hoekenrode 3 1102 BR Amsterdam – Zuidoost Netherlands Telephone number: +31 20 530 4488 email: gdpr@geant.org
Jurisdiction	**Netherlands**

	Dutch Data Protection Authority Autoriteit Persoonsgegevens Postbus 93374 2509 AJ DEN HAAG. Telephone number: (+31) – (0)70 – 888 85 00.

Updated, November 2018