DRAFT: eduTEAMs Privacy Policy

Author(s): SURFnet

Version: 1.0

Date: March 2015

Radboudkwartier 273
3511 CK Utrecht
The Netherlands

PO Box 19035
3501 DA Utrecht
The Netherlands

+31 (0) 30 2 305 305
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
C of C Utrecht 30090777
VAT NL 0089.60.173.B01

Contents

1 Introduction

SURFnet has set up the eduTEAMs service for the purpose of realising optimum cooperation not only amongst the organisations affiliated with SURFnet, but also between these organisations and the information and service providers that have joined eduGAIN. This service consists of various components, including federated authentication and central group management.

SURFnet strives to provide eduTEAMs with the highest possible quality level. In doing so, an important point requiring attention is the integrity of the data of the user and the manner in which Service Providers and SURFnet acting as 'processors' handle the personal data of the user.

1.1 Group Management and Authorisation

eduTEAMs is a self-service group management service that allows end-users whose Identity Providers are part of eduGAIN to create and manage groups and group membership. eduGAIN interconnects identities from national federations, providing a foundation for eduTEAMs to support the international collaboration of groups or teams. The intent for eduTEAMs is to allow group memberships, as created and stored within eduTEAMs, to be used by eduGAIN-registered services to make authorization decisions for those services. The design of the service operates on the basis of the absolute minimal release of attributes: it only releases the group membership attribute for a user that is known at the requesting Service.

Privacy protection
This Policy elaborates in greater detail the most important aspects of privacy protection. An important premise to this Policy is that all parties involved will comply with the applicable legislation and regulations in the field of the protection of privacy and personal data.

The description of the objective(s) for which personal details are processed in the context of eduTEAMs will, in any case, be addressed, as well as on the basis thereof the restrictions in the use of and access to the data.

Transparency for the User is also an important point requiring attention. In addition, retention periods for personal data have been set and the level of security will be developed so as to prevent the abuse of data.

The Privacy Policy is based on the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens* or 'Wbp'). Extensive notes to the Wbp can be found on the site of the Dutch Data Protection Authority: http://www.cbpweb.nl/

2 Federated authentication and group management

The most important functionality of federated authentication is that a User with the electronic identity obtained from his/her own Organisation or other Identity Providers can gain access to services from other organisations or from external Service Providers. For end-users to be able to use eduTEAMs, their Identity Provider must be registered with eduGAIN. By means of central group management, eduTEAMs provides the option of using group accounts in services of various providers. eduTEAMs enables the exchange of supplemental data, group membership and group roles, as a result of which it is possible to integrate services and for Users to work together.

The exchange between the participants in eduTEAMs is described in detail as notes to this Policy on the eduTEAMs website (https://www.eduTEAMs.org). These notes clearly show the manner in which and at which moments personal data are exchanged between which parties.

Aside from SURFnet, which acts as operator of eduTEAMs, the Organisations participating in eduTEAMs can perform the following roles (simultaneously). Privacy obligations that vary per role are described separately in this document.

Role	Description
Identity Provider	an Organisation registered with eduGAIN that provides the data on the identity of the User, making authentication of the User possible.
Attribute provider	an Organisation that provides supplemental personal data on Users.
Service Provider	a service supplier that has registered with eduTEAMs and eduGAIN.

3 Privacy provisions

3.1 What is the aim of data processing?

Central to European and Dutch regulations for the protection of personal data is the principle of purpose limitation; personal data may be processed only to the extent necessary for the realisation of a goal. This goal must be formulated in advance. The law prescribes that the goal must be specified, expressly described and justified. The personal data will not be reused for a goal that is not compatible therewith.

The Identity Provider

In the case of the eduTEAMs service, eduTEAMs acts as a Service Provider towards Identity Providers and personal data is collected by eduTEAMs to provide end-users with functionality to create and manage groups. The data collected is not provided to any third parties, including Services that consume group membership information from eduTEAMs. In addition group membership information is stored for end-users.
As part of the management of group memberships, the administrator of a group (the end-user that created the group) must select which Services are eligible to receive the group membership information. An end-user who is a member of the group must consent to the release of the group membership information towards a specific Service Provider

Within the context of the eduTEAMs service, the Identity provider has a direct relation with the Service Providers that consume eduTEAMs group membership information. eduTEAMs is not providing any personal data that was received from an Identity Provider as part of the authentication process for the eduTEAMs service itself.

The Service Provider receives data from eduTEAMs for:

- the authorisation of a User that desires to obtain access to the service provided by the Service Provider;
- the group memberships of a User if such is required for cooperation and authorisation within the service provided;

An important point of departure here is that the Service Provider processes the group membership data received from eduTEAMs solely on the instruction of the Attribute Provider and/or User. Processing by the Service Provider of the group membership data obtained is based on the assumption that this takes place solely to the extent necessary for the provision of the service. This also includes the communication regarding the service that the User is using or buying, the personalisation of the service and possible invoicing for the use thereof.

Attribute Provider

Towards a Service Provider, eduTEAMs acts as an Attribute Provider offering the ability to a service to query group membership information of a specific user. To be able to query this information, the Service must have obtained an identifier for the given user via the users Identity provider beforehand. A Service Provider can only obtain group membership information if the administrator of the group in eduTEAMs has allowed the Service to access the group information for that specific group.

SURFnet

SURFnet acts as Operator of eduTEAMs and forwards the group account data to the Service Providers. In this process, the Operator acts as a conduit: it is in fact the User himself/herself that consents to furnishing the Service Provider with data.

SURFnet will store personal data to ensure that the services of various Service Providers can be used via eduTEAMs. Examples of this include the following:

- Upon registration of the User's declarations of consent;
- Upon recording which services a User is using;
- Group accounts for Users that want to form groups to be able to work together.

It also applies in this context that SURFnet will process the data solely to the extent necessary for the provisioning of eduTEAMs service. SURFnet will not use the personal data for its own purposes or provide third parties therewith without the consent of the Organisation.

Log files

Aside from processing data for the purpose of rendering the service, the Service Provider and SURFnet will store data in log files. The purpose of these log files is limited to the management of the service, the internal audit of the processes, security and possibly dispute handling.

3.2 User Consent

As regards the processing of personal data, the User is requested by eduTEAMs to grant consent to forward these data to the Service Provider as soon as:

- It approaches a service the first time;
- Conditions are changed.

After 6 months of inactivity on the part of a User, that User will automatically be de-provisioned at eduTEAMs. If, however, the User desires to use the services via eduTEAMs again, consent for the release of data will have to be requested once again. The same is true after the User has initiated the de-provisioning procedure at a moment of his/her choosing.

SURFnet sets out clearly which data are to be released to which Service Provider. In the process, the assumption is always that only those data are released that are necessary for the proper functioning of a service.

The User has an eduTEAMs profile page where consent for the release of attributes can be given and revised, the profile can be deleted and the used attributes per service can be reviewed.

3.3 Which data is recorded?

Privacy legislation sets the requirement for the collection of data that not too many or too detailed data are collected (not excessively), that the data are sufficient (so that no incorrect/incomplete picture arises) and are relevant (not superfluous).

When processing personal data, Identity Providers, Attribute Providers and Service Providers will have to ask the question at all times whether or not the same goal could be reached with fewer data.

SURFnet defines a minimum (mandatory) set of attributes that are necessary for the use of eduTEAMs. The data must be correct and precise. That means that when his/her data are first recorded, the User is identified and that periodic internal or external audits are necessary to verify whether data are still correct.

The nature of some personal data entails that the processing thereof can form a major intrusion of the privacy of the person concerned, such as his/her religion, race, political inclinations, health and criminal history. For this reason, Dutch law features a stricter regime with respect to these data, whereby the point of departure is that these 'special' data may not be processed. Needless to say, a number of specific exceptions from this prohibition exist in this law. For eduTEAMs, it applies that no participant will process special data except with the express consent of the User.

The Identity Provider

In the context of providing service via eduTEAMs, the Organisation will process the following data:

- A persistent identifier for the user, in the form of the eduPersonPrincipleName attribute
- The email address of the user, in the form of the Mail attribute
- The name of the user, in the form of the Displayname attribute

Attribute Provider

In the context of providing the service, eduTEAMs will process the following data:

- Data for User authentication.
  The basis for authentication is the user data received from the Identity Provider as describe in the section above.
- Data for communication (e.g. e-mail address);
  A user will be notified via email when:
  - a team admin invites the user to join a team
  - a team admin remindes the user of the pending invite to join a team
  A team admin will receive an email when:
  - A user requests to join a team
- Data containing group membership information
  Group membership information will be provided in the form of the IsMemberOf attribute in case of a SAML attribute query, or as part of the group statement in case of a VOOT API call.

The Service Provider

The Service Provider will process the data or the categories thereof and possibly store them.

It is possible that the Service Provider will collect data to maintain a User profile, so that a User, for instance, when logging in again, can see what he/she did the previous time (such as a shopping basket for a web shop that has not been checked out or search operations that are being kept).

SURFnet

In addition to the transaction and session data, the operator stores User profile data in his/her log files. If a user uses group management, team member data will also be stored as well as his/her own profile data. When accepting the invitation to become a member of a team, these team members must give their consent to their data being shared.

3.4 Where are the data processed?

It is important that the personal data are processed solely in countries with an appropriate level of protection.

Currently, the eduTEAMs service as operated by SURFnet processes data solely in the Netherlands. If this were to change, SURFnet will incorporate into this Policy where the processing takes place, whereby of course only those countries with an appropriate level of protection will qualify. The eduTEAMs service abides by the eduGAIN Data Protection Code of Conduct.

> "The Data protection Code of Conduct describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management. The Data protection Code of Conduct defines behavioural rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organisations. It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct." -- http://www.geant.net/uri/dataprotection-code-of-conduct/v1/Pages/default.aspx

The eduTEAMs service cannot guarantee group membership data is only provided to Service Providers in countries with an appropriate level of protection.

Therefore, in accordance with the eduGAIN Code of Conduct, the eduTEAMs service will always ask for end-user consent before providing group membership data towards Service Providers. This consent will be requested per team, upon becoming a member of that specific team.

3.5 Who is furnished with the data?

The Identity Provider

The data that have specifically been included for the User to obtain services are issued solely to the eduTEAMs service to grant access and to perform the service.

Attribute Provider

The attribute provider delivers the group membership statement for a specific user towards a requesting Service Provider

The Service Provider and SURFnet

It is only with the unequivocal consent of the Users that the personal data are issued to third parties, unless it concerns a lawful request from an authorised national authority and there is an obligation to render cooperation. In that case, the Service Provider or SURFnet will inform the persons concerned. Attempts will be made to keep access restricted as much as possible.

Only the User has access to possible User profiles to the extent the profiles have not been anonymised.

For the purpose of gaining insight into the service, for instance to generate user statistics, the data can be issued in an anonymous form.

3.6 How is transparency for the User realised?

An important goal of the Dutch Personal Data Protection Act concerns transparency. For the privacy of the Users to be properly protected, it is necessary that the User has insight into what happens with his/her personal data. The more sensitive the data for the User, the more reasons there are to inform the User in detail regarding the processing of his/her data.

For the promotion of this transparency, the Personal Data Protection Act imposes a number of obligations on the person responsible and grants a number of rights to the persons concerned. The Service Providers and SURFnet will render their cooperation to ensure that the persons concerned are able to exercise their right to inspection and correction.

The Service Provider

The Service Provider receives the data from the User during the process that eventually leads to access and use of the service offered by the Service Provider. The Service Provider will ensure that when using the services of the Service Provider, the User is informed of the manner in which the Service Provider handles the personal data. Service Providers often have their own privacy regulations. They will be requested to make these regulations available to the User.

SURFnet

This Privacy Policy describes as well as possible how SURFnet handles personal data.

In addition, all of SURFnet's services are covered by so-called conditions of use containing privacy provisions. These conditions of use can be viewed by clicking the applicable option when the User wants to make use of a SURFnet service.

SURFnet provides Users with a profile page where consent for the release of attributes can be given and revised, the profile can be deleted and the used attributes can be viewed per service.

3.7 How are the personal data secured?

The Personal Data Protection Act makes reference to an appropriate level of security against loss or any form of unlawful processing of personal data. In this connection, the term 'an appropriate level of security' indicates that a consideration is made between the security efforts to be made and the sensitivity of the personal data.

SURFnet security policies apply; those policies may be reviewed upon request.

If SURFnet engages subcontractors in the performance of its services for hosting eduTEAMs, they will enter into an agreement with the subcontractor containing confidentiality and security obligations.

3.8 What is the retention period and when are data deleted?

The general rule is that personal data may not be retained longer than necessary for the purpose for which the data are collected.

SURFnet

SURFnet will not retain any data regarding Users of the Organisation or other Identity Providers/Attribute Providers present within eduTEAMs longer than 6 months after the last transaction. Afterwards it will delete all data from the systems.

The personal data in the log files of SURFnet will be retained for no more than 7 months (one month longer than mentioned above to ensure the last transaction up to 6 months back can be traced).

The Service Provider

The personal data will be retained for no longer than 6 months after the last transaction of the User. Afterwards the data will be deleted from the systems. Before that is done, the Users will be given the opportunity to retrieve the stored data with due observance of a reasonable period.