
# SURFconext Privacy Policy

Author(s): SURFnet

Version: 2.1

Date: August 2017

Moreelsepark 48
3511 EP Utrecht
The Netherlands

PO Box 19035
3501 DA Utrecht
The Netherlands

+31 (0) 88 - 787 30 00
info@surfnet.nl
www.surf.nl/surfnet

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

# Contents

# 1 Introduction

SURFnet established the SURFconext service to ensure optimal cooperation between the institutions connected to SURFnet (hereinafter referred to as the Institution) and with the information and service providers. This service consists of various components, which can be found on the services page: https://www.surf.nl/en/services-and-products/surfconext/what-is-surfconext/index.html .

SURFnet aims to provide SURFconext at the highest possible quality level. It is important to consider user data integrity and the way Service Providers and SURFnet handle Users' personal data as "processors".

## 1.1 Trust framework

SURFconext uses a so-called "trust framework". SURFconext participants belong to this trust framework if they subscribe to a set of arrangements that offer security in terms of data integrity and user privacy as described in this Privacy Policy.

When Service Providers with a commercial interest or Service Providers not belonging to the SURFnet target group join, contractual arrangements that include this Privacy Policy will be established.

Arrangements with the Institutions are made and documented in an Annex to the SURFnet User Agreement. This Policy is also used as the foundation of these arrangements in terms of privacy.

SURFnet will sign a separate agreement based on the provisions of this Privacy Policy with the other SURFconext participants, including the Virtual Organisations and Attribute Providers.

This Policy also defines how SURFnet handles personal data in its capacity as operator.

SURFconext also has participants who are unable or unwilling to subscribe to the trust framework. Institutions should always check the (privacy) conditions for the service offered by the relevant participant. It is possible to make additional one-to-one arrangements.

## 1.2 Privacy protection

This Policy develops the key aspects of privacy protection further. One important premise for this Policy is that all parties involved adhere to the applicable privacy and personal data protection laws and regulations.

The Policy describes the reason(s) why personal data are processed as part of SURFconext and how the use of and access to that data is restricted. Transparency to the User is also an important area to consider. Personal data retention periods are defined and a security level is developed to prevent any unauthorised use of the data.

The Privacy Policy is based on the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens or "Wbp"). Extensive notes to the Personal Data Protection Act can be found on the Dutch Data Protection Authority's website.

# 2 Federated authentication

The key functionality of federated authentication as offered by SURFconext is that Users with digital identities obtained from their own Institutions or other Identity Providers can access the services offered by Service Providers connected to SURFconext.

The SURFconext federated authentication service constitutes a central hub for handling and directing all login requests. This means that Institutions are not required to setup and manage connections to all Service Providers: a single connection with the hub is sufficient to access all connected Service Providers. SURFconext makes it possible to exchange additional data, so services can integrate and that Users can work together.

The exchange of information between the participants in SURFconext is described in detail on the SURFnet website (https://profile.surfconext.nl/). On that website, users can see which personal data was exchanged with which parties (in the form of attributes).

SURFnet acts as the SURFconext operator. Organisations participating in SURFconext can fulfil the following roles (one or more per organisation). If the privacy requirements are different for each role, they will be described separately in this document.

| | |
|---|---|
| Identity Provider | An organisation providing data on the User's identity in order to allow User authentication |
| Attribute Provider | An organisation providing additional data about the User |
| Service Provider | An organisation that is connected to SURFconext and provides services |

# 3 Privacy provisions

## 3.1 What is the purpose of processing the data?

The European and Dutch personal data protection regulations are based on the purpose limitation principle: personal data can only be processed if they are necessary to achieve a specific purpose. This purpose must be described in advance. A specific description and justification of the purpose are required by law. The personal data will not be used again for any other incompatible purpose.

**The Identity Provider & Attribute Provider**

The Identity Provider – the Institution, for example – often has account data. These account data will be used to give Users access to the range of services offered via SURFconext. As far as the use of the services is concerned, additional User data may be collected for each service if this is necessary to personalise a certain service or provide access to it. These additional data may be provided by the Identity Provider, added to profiles by the Users themselves and/or obtained from an Attribute Provider.

If the Institution or another Identity Provider/Attribute Provider collects User data for a purpose that was already determined before the participation in SURFconext, the Identity Provider/Attribute Provider must ensure that any data provided to SURFnet as part of the SURFconext connection must be in line with this purpose. Data can only be added to this specific SURFconext administration if the data are in line with this purpose.

**The Service Provider**

The Service Provider obtains data from the Identity Provider/Attribute Provider for:

- Authentication (proof of authentication by the Identity Provider)
- Authorisation of a User trying to access the service offered by the Service Provider
- Group memberships of a User if required for working together and authorisation within the service provided
- Extra data from a User relevant to its service

It is important to consider that the Service Provider only processes the personal data on behalf of the Identity Provider/Attribute Provider and/or User. The principle is that the Service Provider only processes the obtained data if it is necessary to provide the service. This includes communication concerning the services provided to the User, personalisation of the service and any billing for the use of services.

**SURFnet**

SURFnet acts as the Operator of SURFconext and forwards data on the User and group relations to the Service Providers. The Operator acts as an intermediary in this process. The Identity Provider/Attribute Provider and/or the Users themselves are the ones who actually provide the data to the Service Provider.

SURFnet will save personal data to allow the services offered by various Service Providers via SURFconext. For example:

- Upon registration of the User's declaration of consent

- Upon registration of the services a User has logged on to
- Group relations for Users who want to form groups in order to work together

Again, SURFnet will only process the data if they are necessary for the delivery of SURFconext. SURFnet will only use the personal data on behalf of the Institution and/or User and according to the instructions of the Institution and/or User. SURFnet will not use the personal data for its own purpose and will not provide the personal data to any third parties without the consent of the Institution and/or User.

**Log files**

In addition to data processing for services, the Service Provider and SURFnet will save data in log files. The purpose of these log files is limited to service management, internal process control, security and, where appropriate, the handling of disputes.

## 3.2 User consent

SURFnet asks for the User's consent to forward the personal data it processes to the Service Provider:

- When the User approaches a service for the first time
- When a changed attribute is provided

The User's consent request as described above can be disabled at the Institution's request.

SURFnet sets out clearly which data are to be released to which Service Provider. When a service connects to SURFconext, the Service Provider will be reminded only to request the data that are necessary for the smooth operation of the service.

The User has a SURFconext profile page, which contains the used attributes per service, for example.

## 3.3 Which data are saved?

Privacy legislation requires that the quantity and detail of the data collected is limited (not excessive) and the data are sufficient (to avoid incorrect/incomplete information) and relevant (not superfluous).

When Identity Providers, Attribute Providers and Service Providers process personal data, they always need to ask themselves whether less data can be used to achieve the same goal.

SURFnet defines a minimal (mandatory) set of attributes that an Identity Provider should be able to provide and that are necessary for using SURFconext and the connected services. The data must be correct and accurate. This means that the User should be correctly vetted by the Identity Provider when data are initially recorded (provisioned in the identity management system of the Identity Provider). After that, periodic (internal) checks must be performed by the Identity Provider to ensure the data are still correct.

By the very nature of certain personal data, their processing may constitute a major breach of a person's privacy in terms like religion, race, political affiliation, health and criminal history. The law

therefore applies a stricter regime for this type of data. The principle of this regime is that these so-called "special" data must not be processed. Of course, the law provides a number of specific exceptions to this principle. In terms of SURFconext, the rule is that participants can never process any special data unless they have the User's express permission.

**The Identity Provider & Attribute Provider**

In the context of SURFconext services, Identity and Attribute Providers can process the following data:

- Data for User authentication
- Data for communication (e.g. e-mail address)
- Data from which User rights can be derived, provided that these rights are related to the use of the SURFconext services (examples include course programme, faculty and position)

**The Service Provider**

The Service Provider will process and possibly save the data (categories) that were, whether or not via SURFconext, delivered by, and/or created by actions of, the Identity Provider, Attribute Provider and/or User.

The Service Provider may collect data for a User Profile in order to show Users what they were doing the previous time they logged in (cf. an abandoned shopping cart on a web store, saved searches, etc.). SURFconext will always recommend its privacy-friendly solutions for this to the Service Provider.

**SURFnet**

Besides transaction and session data, the operator stores User profile data in its log files. If a User uses central group management or institutional groups, the team members' data will be saved in addition to the User's own profile data. These team members are asked to give their consent to their data being shared when they accept their membership invitation.

## 3.4 Where are the data processed?

SURFnet currently only processes data in the Netherlands. If this were to change, SURFnet will include the processing location in this Policy. Of course, only countries offering the appropriate protection level will be considered.

## 3.5 Who receives the data?

**The Identity Provider & Attribute Provider**

Data specifically included for services received by the User are only provided to the Service Provider that needs these data to give access and perform the services.

**The Service Provider and SURFnet**

Personal data are only provided to third parties when the Users have provided their unambiguous consent, unless a competent national authority issues a legal request and cooperation is mandatory. If this is the case, the Service Provider or SURFnet will inform the parties involved. Access will be kept as limited as possible.

Anonymised data may be provided to offer more insight into the service with user statistics, for example.

## 3.6 How is transparency for the User achieved?

Transparency is an important goal of the Personal Data Protection Act. To ensure adequate User privacy protection, it must be clear for Users what their personal data are used for. The more sensitive the data are to the User, the more reason there is to provide detailed information to the User on the processing of the data.

In order to promote this transparency, the Personal Data Protection Act imposes a number of duties on the data controller and grants a number of rights to the data subjects. The Service Providers and SURFnet will cooperate to ensure that data subjects can exercise their right of access and correction.

**The Service Provider**

The Service Provider obtains the data from the User in a process that eventually leads to the access and use of the service offered by the Service Provider. The Service Provider will ensure that Users of the Service Provider's services are kept informed on how the Service Provider is handling the personal data. Service Providers often have their own privacy rules. They will be asked to make these rules available to the User.

**SURFnet**

This Privacy Policy provides a description of how SURFnet handles personal data.

SURFnet offers Users a profile page where they can revoke their consent for the release of attributes and view the used attributes per service.

## 3.7 How are personal data protected?

The Personal Data Protection Act mentions an appropriate security level against loss or any form of unlawful processing of personal data. The term "appropriate security level" indicates that a balance must be struck between the security efforts to be made and the sensitivity of the personal data.

The SURFconext participants will ensure adequate protection against any loss, damage and unauthorised disclosure or editing of the data.

Adequate means that:

- The security policy of the participants describes the data security level.
- A classification and risk analysis have taken place and the consequences of these have been implemented.
  It is regularly assessed whether the security level of the technology, procedures and work processes is sufficient for the risks associated with the personal data processed.

For institutions of higher education, the possibility exists to participate in the SURFaudit for the purpose of completing the audit referred to above. In that case, the desired outcome is level 3 of the Capability Maturity Model, which is used in the SURFaudit for the standards set in the

"toegangsbeveiliging" (SURFaudit is only available in Dutch) cluster. For information on SURFaudit, see: https://www.surf.nl/en/services-and-products/surfaudit/index.html .

**The Service Provider**

SURFmarket and SURFnet address security of (personal) data in their arrangements with Service Providers. Many security and (personal) data arrangements are best included in the Data Processor Agreement between the Institution and the Service Provider.

**SURFnet**

The security policy of SURFnet's services is documented. The platform used for the SURFconext service is subjected to various types of audit once every two years:

1. Technical security audit
2. Audit of management processes

Audit results will be shared with the Institutions and possibly with other Identity Providers and Attribute Providers.

If the Institutions wish to have an additional audit by an accredited auditor, SURFnet will also arrange this once every three years. The costs of this audit will be charged to the relevant Institution. The Institutions will treat the audit results confidentially and will only share them with SURFnet.

Access to servers running the SURFconext platform is restricted with the SSH network protocol. Server rooms and cabinets are locked at all locations. Access to physical rooms is recorded in log files and is only possible for authorised individuals.

SURFnet will document, analyse and report any security incidents with regard to the SURFnet service and their estimated impact to the parties involved.

**SURFnet and Service Provider**

If the Service Provider or SURFnet engages subcontractors for its services, it will sign an agreement that includes privacy provisions and confidentiality and security obligations with the subcontractors.

## 3.8 What are the retention periods and when are the data deleted ?

As a general rule, personal data must not be saved any longer than necessary in terms of the purpose for which the data were collected.

**SURFnet**

SURFnet will delete all data on Users of the Institution or other Identity Providers/Attribute Providers present in SURFconext at the User's request or automatically 37 months after the last login.

The personal data in SURFnet's log files will be retained for no more than 6 months.

**The Service Provider**

The Institution is responsible for arrangements on retention periods about data processed by Service Providers.