SURFconext Privacy Policy

Author(s):	SURFnet
Version:	2.0
Date:	November 2016

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 3

1.1 Trust framework 3
1.2 Privacy protection 3

2 Federated authentication and group management 5

3 Privacy provisions 6

3.1 What is the aim of data processing? 6
3.2 User Consent 7
3.3 Which data are recorded? 7
3.4 Where are the data processed? 8
3.5 Who is furnished with the data? 9
3.6 How is transparency for the User realised? 9
3.7 How are the personal data secured? 10
3.8 What is the retention period and when are data deleted? 11

1 Introduction

SURFnet has set up the SURFconext service for the purpose of realising optimum cooperation not only amongst the organisations affiliated with SURFnet (hereinafter “the Organisation”), but also between these organisations and information and service providers. This service consists of various components, which can be found on the services page.

SURFnet strives to provide SURFconext 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 ‘processor’ handle the personal data of the user.

1.1 Trust framework

SURFconext features a trust framework. A participant in SURFconext belongs to this trust framework if it endorses a set of arrangements that provide safeguards for the integrity of the data and for the privacy of the user as described in this Privacy Policy.

When Service Providers join that do not belong to the SURFnet target group or have commercial objectives, contractual agreements will have to be laid down with SURFmarket. In contract discussions with a Service Provider, this Privacy Policy will be used as the point of departure to the extent it relates to privacy.

Organisations are bound by agreements that are recorded in an Appendix to the SURFnet user agreement. It also applies to these agreements that this Policy will be used as the point of departure to the extent it relates to privacy. If an Organisation acts as a commercial service provider, the Organisation will be requested to enter into an agreement with SURFmarket such as it is also concluded for the Service Providers outside of the target group.

SURFnet will conclude a separate agreement with other participants in SURFconext, including the Collaborative Organisations and the Attribute Providers, which will contain the provisions from this Privacy Policy as the point of departure.

In addition, this Policy sets out how SURFnet, in its role as operator, handles personal data.

SURFconext also has participants that cannot or do not desire to endorse the trust framework entirely. In those cases, Organisations must check the privacy conditions under which the service is being offered by the relevant participant. Under certain circumstances, it may be possible to make individualised, supplemental agreements. The SURFconext website makes it clear which participants meet the requirements of the trust framework.

1.2 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 SURFconext 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 Dutch Data Protection Authority's website: www.autoriteitpersoonsgegevens.nl.

This Policy will be laid down by SURFnet in consultation with the Organisations.

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.

By means of central group management, SURFconext provides the option of using group accounts in services of various providers.

The federated authentication services of SURFconext are a central gateway through which all log-in requests are handled and sent in the right direction. This way, an Organisation need not link up with all Service Providers itself, but suffices with a single link. A similar advantage applies to the central group management of SURFconext. SURFconext enables the exchange of supplemental data as a result of which it is possible to integrate services and for Users to work together.

> The exchange between the participants in SURFconext is described in detail as notes to this Policy on the SURFnet website (https://profile.surfconext.nl/). These notes clearly show which personal data are exchanged with which parties (in the form of attributes).

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

Role	Description
Identity Provider	an Organisation 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 joined SURFconext. SURFmarket concludes an agreement relating to the provision of the services with parties that offer a commercial service.

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 & Attribute Provider

The Organisation acting as an Identity Provider often disposes of a ‘database of User data’. The data originating from this database will be used to grant Users access to services within their own Organisation and to a range of services made available via SURFconext. In the context of using services, additional User data can be collected per service, if that is necessary for access to or the personalisation of a specific service. These can be extra data from the database of the Organisation and/or extra that a User himself/herself adds to his/her profile and/or data obtained from an Attribute Provider.

If the goal of the database has already been set by the Organisation or another Identity Provider/Attribute Provider prior to participation in SURFconext, the issue of data within the context of SURFconext must be in line with this goal. Besides that, the addition of the data to this database must, specifically for SURFconext, fit within the goal

The Service Provider

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

- the authentication (the proof of authentication by the Identity Provider);
- 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;
- extra data from a User relevant to its service.

An important point of departure here is that the Service Provider processes the personal data solely on the instruction of the Identity Provider/Attribute Provider and/or User. Processing by the Service Provider of the 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 buying, the personalisation of the service and possible invoicing for the use thereof.

SURFnet

SURFnet acts as Operator of SURFconext and forwards the personal data and group accounts to the Service Providers. In this process, the Operator acts as a conduit: it is in fact the Identity Provider/Attribute Provider and/or the User himself/herself that furnishes the Service Provider with data.

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

- Upon registration of the User’s declaration 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 provision of SURFconext. SURFnet will use the personal data solely on the instructions of the Organisation and in compliance therewith. SURFnet will not use the personal data for its own purposes or provide third parties therewith without the consent of the Organisation. The Organisation can grant consent to all Service Providers by consenting to the Opt-out policy. The Opt-out policy can be found at https://support.surfconext.nl. The Organisation can also opt to have this determined per Service Provider.

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 SURFnet to grant consent to forward these data to the Service Provider as soon as:

- it approaches a service the first time;
- conditions are changed.

At the request of an Organisation, the request to the User for consent as described above can be eliminated.

After 6 months of inactivity on the part of a User, that User will automatically be deprovisioned at SURFconext. If, however, the User desires to use the services via SURFconext again, consent for the release of data will have to be requested once again. The same is true after the User has initiated the deprovisioning 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 a SURFconext profile page where the profile can be deleted and the used attributes per service can be reviewed.

3.3 Which data are 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 SURFconext and linked services. 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 in respect of 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 SURFconext, it applies that no participant will process special data except with the express consent of the User.

The Identity Provider & Attribute Provider

In the context of providing service via SURFconext, the Organisation and the other Identity Provider will process the following data (whereby an Attribute Provider only processes a part thereof):

- Data for User authentication.

If necessary for buying the service offered to which the User desires to have access, the following personal data can also be processed:

- Data for communication (e.g. e-mail address);
- Data from which rights of the User can be derived to the extent such rights are related to the use of the services within SURFconext (examples include course of study, faculty or job/position).

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 central group management or Organisation groups, 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. in accordance with European and national privacy legislation.

When the contractual agreements with the Service Providers are recorded by SURFmarket, the approach is that the Service Provider complies therewith and that if it is not or no longer possible to meet this obligation, the right arises to terminate the agreements. Organisations that act as a Service Provider will also have the processing of personal data take place only in countries with an appropriate level of protection.

Currently, 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.

3.5 Who is furnished with the data?

The Identity Provider & Attribute Provider

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

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.

The participants in SURFconext make arrangements for adequate security against loss, damage and unauthorised inspection or modification of the data.

The term ‘adequate’ means that:

- the security policy of the participants includes the extent of security for data;
- a classification and risk analysis have taken place and the consequences thereof have been implemented;
- by means of an independent, regular audit of the security measures, it has been established whether in terms of technology, procedures and work processes security is sufficient for the risks that are taken in keeping personal data;
- Security incidents and their possible impact are noted and, preferably, reported to the persons concerned.

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 ‘access security’ cluster.

For the SURFaudit, see:

https://www.surf.nl/diensten-en-producten/surfaudit/index.htm

The Service Provider

SURFmarket will incorporate into the agreement with the Service Provider the obligation to take adequate security measures against loss or any form of unlawful act. These measures assume that the Service Providers will, upon request, provide insight into the measures they take for the protection of personal data, so that compliance with the obligation to provide adequate security can be monitored.

In addition, the Service Provider will report security incidents and their possible impact.

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; and
2. management processes audit.

The outcomes of audits will be shared with the Organisations and possibly with other Identity Providers and Attribute Providers.

If the Organisations desire to have a supplemental audit performed by a certified auditor, SURFnet will comply therewith once every three years. The costs for this audit will be borne by the relevant

Organisation. The results of the audit will be handled confidentially by the Organisation and shared solely with SURFnet.

Virtual access to servers on which the platform runs is restricted with the aid of the SSH network protocol. Server rooms and server cabinets are locked at all locations. Access to physical rooms is recorded in log files and is only possible for authorised individuals.

If security incidents in respect of SURFnet's services occur, SURFnet will record and analyse them and report as quickly as possible on them, including the estimated impact, to the parties concerned.

SURFnet and Service Provider

If the Service Provider or SURFnet engages subcontractors in the performance of its services, they will enter into an agreement with the subcontractor containing privacy provisions and 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 delete all data regarding Users of the Organisation or other Identity Providers/Attribute Providers present within SURFconext at the User's request (via the profile page), or else automatically 37 months after the last log-in.

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

The Service Provider

The retention periods will be agreed with each Service Provider. The assumption here is that personal data will not be retained any longer than necessary. Before that is done, the Users will be given the opportunity to retrieve the stored data with due observance of a reasonable period.