Privacy policy SURFconext

Auteur: SURFnet

Versie: 2.2

Datum: 23 Oktober 2018

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

+31-887873000
info@surfnet.nl
www.surfnet.nl

Deutsche Bank 46 57 33 506
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

1 Inleiding

Ten behoeve van een optimale samenwerking tussen de bij SURFnet aangesloten instellingen (hierna de Instelling) onderling en met informatie- en dienstenleveranciers, heeft SURFnet de SURFconext dienst opgezet. Deze dienst bestaat uit verschillende componenten, die te vinden zijn op de dienstenpagina. [1]

SURFnet streeft er naar om SURFconext met een zo hoog mogelijk kwaliteitsniveau te leveren. Een belangrijk aandachtspunt hierbij is de integriteit van de gegevens van de gebruiker en de wijze waarop Service Providers en SURFnet als 'verwerker' met persoonsgegevens van de gebruiker omgaan.

1.1 Trust framework

SURFconext kent een zogenaamd 'trust framework'. Een deelnemer aan SURFconext behoort tot dit 'trust framework' indien hij een set van afspraken onderschrijft die waarborgen bieden voor de integriteit van de gegevens en voor de privacy van de gebruiker zoals omschreven in deze Privacy Policy.

Bij het aansluiten van Service Providers die commerciële doelstellingen hebben, zullen contractuele afspraken worden vastgelegd waarin deze Privacy Policy wordt meegenomen.

Met de Instellingen worden afspraken gemaakt die zijn vastgelegd in een Bijlage bij de SURFnet Gebruiksovereenkomst. Voor deze afspraken geldt tevens dat, voor zover het de privacy betreft, deze Policy als uitgangspunt dient.

Met overige deelnemers aan SURFconext, waaronder ook de Virtuele Organisaties en de Attribute Providers vallen, zal SURFnet een aparte overeenkomst afsluiten waarin de bepalingen uit deze Privacy Policy als uitgangspunt worden genomen.

Daarnaast is in deze Policy vastgelegd hoe SURFnet in haar rol als operator omgaat met persoons-gegevens.

SURFconext kent ook deelnemers die het 'trust framework' niet geheel kunnen of willen onderschrijven. Instellingen dienen altijd na te gaan onder welke (privacy)voorwaarden de dienst door de betreffende deelnemer wordt aangeboden. Eventueel kunnen één op één aanvullende afspraken worden gemaakt.

1.2 Privacybescherming

In deze Policy worden de belangrijkste aspecten van privacybescherming nader uitgewerkt. Een belangrijke vooronderstelling bij deze Policy is dat alle betrokken partijen de toepasselijke wet- en regelgeving op het gebied van de bescherming van de privacy en persoonsgegevens zullen naleven.

Aan de orde komen in ieder geval de omschrijving van de doel(en) waarvoor persoonsgegevens worden verwerkt in het kader van SURFconext en aan de hand daarvan de beperkingen in het gebruik van en toegang tot de gegevens. De transparantie voor de Gebruiker is daarnaast een belangrijk aandachtspunt. Tevens zijn bewaartermijnen voor persoonsgegevens vastgesteld en wordt er een uitwerking gegeven aan het beveiligingsniveau om misbruik van de gegevens te voorkomen.

[1] https://www.surf.nl/diensten-en-producten/surfconext/wat-is-surfconext/index.html

De Privacy Policy is gebaseerd op de Algemene Verordening Gegevensverwerking (AVG). Uitgebreide toelichting op de AVG is te vinden op de site van de Autoriteit Persoonsgegevens.

2 Federatieve authenticatie

De belangrijkste functionaliteit van federatieve authenticatie zoals SURFconext die biedt, is dat een Gebruiker met de digitale identiteit die is verkregen bij de eigen instelling of overige Identity Providers toegang kan krijgen tot diensten van op SURFconext aangesloten Service Providers.

De federatieve authenticatiedienst van SURFconext vormt een centraal knooppunt waarlangs alle inlogverzoeken worden afgehandeld en de juiste kant op worden gestuurd. Zo hoeft een Instelling niet zelf met alle Service Providers te koppelen, maar volstaat één koppeling. SURFconext maakt het mogelijk aanvullende gegevens uit te wisselen.

Als toelichting bij deze Policy is op de SURFnet website https://profile.surfconext.nl de uitwisseling tussen de deelnemers aan SURFconext in detail omschreven waarbij duidelijk wordt met welke partijen welke persoonsgegevens, in de vorm van attributen, worden uitgewisseld.

Naast SURFnet die optreedt als operator van SURFconext kunnen de aan SURFconext deelnemende organisaties de volgende rollen (naast elkaar) vervullen. Indien de privacyverplichtingen per rol verschillen, zijn ze in dit document apart beschreven.

Identity Provider	een organisatie de gegevens verstrekt over de identiteit van de Gebruiker waardoor authenticatie van de Gebruiker mogelijk is.
Attribute provider	een organisatie die aanvullende gegevens verstrekt over Gebruikers.
Service Provider	dienstaanbieder aangesloten op SURFconext.

3 Privacy-bepalingen

3.1 Wat is het doel van de gegevensverwerking?

In de Europese en Nederlandse regelgeving voor de bescherming van persoonsgegevens staat het principe van de doelbinding centraal; persoonsgegevens mogen slechts worden verwerkt voor zover noodzakelijk ter realisatie van een doel. Het doel moet vooraf worden geformuleerd. De AVG schrijft voor dat de doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. De persoonsgegevens zullen niet opnieuw worden gebruikt voor een doel dat daarmee niet verenigbaar is.

De Identity Provider & Attribute Provider

De Identity provider, bijvoorbeeld de Instelling, beschikt vaak over accountgegevens. Deze gegevens zullen worden gebruikt om Gebruikers toegang te verlenen tot het dienstenaanbod ontsloten via SURFconext. In het kader van het gebruik van diensten kunnen per dienst nog extra gegevens van Gebruikers worden verzameld, indien dat voor toegang tot of personalisatie van een bepaalde dienst noodzakelijk is. Dit kunnen extra gegevens zijn die de Identity provider aanlevert, en/of extra gegevens die een Gebruiker zelf toevoegt aan zijn/haar profiel en/of gegevens die worden verkregen van een Attribute Provider.

De Instelling of andere Identity Provider/Attribute Provider draagt er zorg voor dat een verstrekking van gegevens aan SURFnet, in het kader van de SURFconext-aansluiting, in lijn is met vooraf

vastgelegde doelstellingen rond het verzamelen en verwerken van Gebruikersgegevens. Daarnaast moet het toevoegen van gegevens aan deze administratie specifiek voor SURFconext passen binnen die doelstelling.

De Service Provider

De Service Provider verkrijgt gegevens van de Identity Provider/Attribute Provider ten behoeve van:

- De authenticatie (het bewijs van authenticatie door de Identity Provider).
- Autorisatie van een Gebruiker die toegang wil verkrijgen tot de door de Service Provider verleende dienst.
- Groepslidmaatschappen van een Gebruiker, als dat nodig is voor samenwerking en autorisatie binnen de verleende dienst.
- Extra gegevens van een Gebruiker relevant voor haar dienstverlening.

Belangrijk uitgangspunt hierbij is dat de Service Provider de persoonsgegevens uitsluitend verwerkt in opdracht van de Identity Provider/Attribute Provider en/of Gebruiker. Uitgangspunt hierbij is dat de Service Provider de gegevens die worden verkregen uitsluitend verwerkt voor zover noodzakelijk voor de verlening van de dienst, daaronder valt ook de communicatie over de diensten die de Gebruiker afneemt, personalisatie van de dienst en eventuele facturering van het gebruik.

SURFnet

SURFnet treedt op als Operator van SURFconext en geeft gegevens over de Gebruiker en groepsrelaties door naar de Service Providers. In dit proces fungeert de Operator als een doorgeefluik, het is in feite de Identity Provider/Attribute Provider en/of de Gebruiker zelf die gegevens verstrekken aan de Service Provider.

SURFnet zal persoonsgegevens opslaan om het gebruik van services van verschillende Service Providers via SURFconext mogelijk te maken. Bijvoorbeeld:

- Bij het vastleggen van de toestemmingsverklaring van de Gebruiker.
- Bij het vastleggen op welke diensten een Gebruiker is ingelogd.
- Groepsrelaties voor Gebruikers die groepen willen vormen om samen te kunnen werken.

Ook hierbij geldt dat SURFnet de gegevens uitsluitend zal verwerken voor zover noodzakelijk voor het leveren van SURFconext. SURFnet zal de persoonsgegevens slechts in opdracht en in overeenstemming met de instructies van de Instelling en/of Gebruiker gebruiken. SURFnet zal de persoonsgegevens niet voor eigen doeleinden gebruiken of aan derden verstrekken zonder toestemming van de Instelling en/of Gebruiker.

Logfiles

Naast de verwerking van gegevens ten behoeve van de dienstverlening zullen de Service Provider en SURFnet gegevens opslaan in logfiles. De doelstelling van deze logfiles is beperkt tot het beheer van de dienst, interne controle van de processen, beveiliging en eventueel het behandelen van geschillen.

3.2 Toestemming van de Gebruiker

Voor wat betreft de verwerking van persoonsgegevens wordt door SURFnet aan de Gebruiker om toestemming gevraagd voor het doorgeven van deze gegevens aan de Service Provider:

- zodra deze een dienst de eerste keer benadert,
- bij gewijzigde attribuut doorgifte.

Op verzoek van instelling kan de vraag aan de Gebruiker om toestemming zoals hier boven beschreven worden uitgezet.

SURFnet maakt inzichtelijk welke gegevens aan welke Service Provider wordt vrijgegeven. Bij het op

SURFconext aansluiten van een dienst zal de Service Provider gemaand worden alleen die gegevens te vragen die noodzakelijk zijn voor het goed functioneren van een dienst.

De Gebruiker beschikt over een SURFconext profielpagina waar ondermeer de gebruikte attributen per dienst kunnen worden ingezien.

3.3 Welke gegevens worden vastgelegd?

In de AVG wordt aan het verzamelen van gegevens de eis gesteld dat er niet te veel of te zeer gedetailleerde gegevens worden verzameld (niet bovenmatig), dat de gegevens toereikend zijn (zodat er geen verkeerd/onvolledig beeld ontstaat) en ter zake dienend zijn (niet overbodig).

Identity Providers, Attribute Providers en Service Providers zullen zich bij het verwerken van persoonsgegevens steeds de vraag moeten stellen of er niet met minder gegevens hetzelfde doel bereikt kan worden.

SURFnet definieert in overleg met de betrokken partijen per Service Provider een minimale (verplichte) set attributen die nodig zijn om gebruik te kunnen maken van SURFconext en gekoppelde services. De gegevens moeten juist en nauwkeurig zijn. Dat betekent dat de Gebruiker bij eerste opname van de gegevens is geïdentificeerd en dat er periodieke (interne) controles nodig zijn om na te gaan of gegevens nog juist zijn.

De aard van sommige persoonsgegevens brengt met zich mee dat verwerking ervan een grote inbreuk kan vormen op de privacy van de betrokkene zoals godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden. Daarom kent de AVG voor deze gegevens een strenger regime, waarbij het uitgangspunt is dat deze zogenaamde ‘bijzondere’ gegevens niet mogen worden verwerkt. Uiteraard kent de AVG een aantal specifieke uitzonderingen voor dit verbod. Voor SURFconext geldt dat er door alle deelnemers geen bijzondere gegevens zullen worden verwerkt behalve met uitdrukkelijke toestemming van de Gebruiker.

De Identity Provider & Attribute Provider

In het kader van de dienstverlening middels SURFconext kunnen Identity- en Attribute Providers de volgende gegevens verwerken (waarbij een Attribute Provider slechts een deel verwerkt):

- Gegevens voor authenticatie van Gebruikers.
- Gegevens voor communicatie (bijv. e-mailadres)
- Gegevens waaruit bevoegdheden van de Gebruiker kunnen worden afgeleid voor zover deze verband houden met het gebruik van de services binnen SURFconext (denk aan studierichting, faculteit, functie, etc.).

De Service Provider

De Service Provider zal de (categorieën van) gegevens verwerken en eventueel opslaan die de door de Identity Provider, Attribute Provider en Gebruiker, al dan niet via SURFconext, zijn aangeleverd en/of ontstaan door hun acties.

Het is mogelijk dat de Service Provider gegevens verzamelt om een Gebruikersprofiel bij te houden, zodat een Gebruiker bij hernieuwd inloggen bijvoorbeeld kan zien wat zij/hij de vorige keer heeft gedaan (vgl. een boodschappenmandje bij een webwinkel dat nog niet is afgerekend, zoekacties die worden bewaard, etc.). SURFconext beschikt over privacy-vriendelijke oplossingen daarvoor, en zal die altijd aanraden aan de Service Provider.

SURFnet

De operator slaat naast de transactie- en sessiegegevens in haar logfiles profielgegevens van de Gebruiker op. Indien een Gebruiker gebruik maakt van centraal groepsmanagement of instellingsgroepen, worden naast de eigen profielgegevens ook gegevens van teamleden opgeslagen. Deze teamleden dienen bij de aanvaarding van de uitnodiging voor lidmaatschap van een team

akkoord te gaan met het delen van hun gegevens.

3.4 Waar worden de gegevens verwerkt?

De verwerking van gegevens door SURFnet vindt momenteel uitsluitend plaats in Nederland. Mocht dit wijzigen dan zal SURFnet in deze Policy opnemen waar de verwerking plaatsvindt waarbij uiteraard alleen landen met een passend beschermingsniveau in aanmerking komen.

3.5 Aan wie worden de gegevens verstrekt?

De Identity Provider & Attribute Provider

De gegevens die specifiek zijn opgenomen ten behoeve van het afnemen van diensten door de Gebruiker worden uitsluitend verstrekt aan de Service Provider die deze gegevens nodig heeft voor het verlenen van toegang en het uitvoeren van de dienst.

De Service Provider en SURFnet

Alleen met ondubbelzinnige toestemming van de Gebruikers worden de persoonsgegevens verstrekt aan derden, tenzij het een rechtmatig verzoek betreft van een bevoegde nationale autoriteit en er een verplichting is tot medewerking. Indien dat het geval is zal de Service provider of SURFnet de betrokkenen indien mogelijk informeren. Getracht zal worden de toegang zo beperkt mogelijk te houden.

Voor het verkrijgen van inzicht in de dienst, bijvoorbeeld voor het genereren van gebruiksstatistieken kunnen de gegevens geanonimiseerd worden verstrekt.

3.6 Hoe wordt transparantie voor de Gebruiker bewerkstelligd?

Een belangrijke doelstelling van de AVG betreft de transparantie. Voor een goede bescherming van de privacy van de Gebruikers is het noodzakelijk dat de Gebruiker inzicht heeft in wat er gebeurt met zijn/haar persoonsgegevens. Hoe gevoeliger de gegevens voor de Gebruiker zijn, hoe meer reden er is om de Gebruiker gedetailleerd te informeren over de gegevensverwerking.

De AVG legt ter bevordering van deze transparantie een aantal plichten bij de verwerkings-verantwoordelijke en een aantal rechten bij de betrokkenen. De Service Providers en SURFnet zullen hun medewerking verlenen om zeker te stellen dat betrokkenen hun recht op o.a. inzage en correctie kunnen uitoefenen.

De Service Provider

De Service Provider verkrijgt de gegevens van de Gebruiker gedurende het proces dat uiteindelijk leidt tot toegang en gebruik van de door de Service Provider aangeboden dienst. De Service Provider zal er zorg voor dragen dat de Gebruiker bij gebruik van de diensten van de Service Provider op de hoogte wordt gesteld van de wijze waarop de Service Provider met persoonsgegevens omgaat. Service Providers hebben vaak een eigen privacyreglement. Aan hen zal gevraagd worden om dit reglement toegankelijk te maken voor de Gebruiker.

SURFnet

In deze Privacy Policy wordt zo goed mogelijk omschreven hoe SURFnet omgaat met de persoonsgegevens.

SURFnet biedt de Gebruiker een profielpagina waar ondermeer toestemming voor het vrijgeven van attributen herzien kan worden en de gebruikte attributen per dienst ingezien kunnen worden.

3.7 Hoe worden de persoonsgegevens beveiligd?

In de AVG wordt gesproken van een passend beveiligingsniveau tegen verlies of tegen enige vorm van onrechtmatige verwerking van persoonsgegevens. De term een passend beveiligingsniveau geeft in dit verband aan dat een afweging wordt gemaakt tussen de te leveren beveiligingsinspanning en de gevoeligheid van de persoonsgegevens.

De deelnemers aan SURFconext dragen zorg voor een adequate beveiliging tegen verlies, beschadiging en ongeoorloofde kennisneming of aanpassing van de gegevens.

Met adequaat wordt bedoeld dat:

- Het beveiligingsbeleid van de deelnemers een uitspraak doet over de mate van beveiliging van gegevens.
- Een classificatie en risicoanalyse hebben plaatsgevonden en de consequenties daarvan zijn geïmplementeerd.
- Regelmatig wordt beoordeeld of beveiliging op de punten techniek, procedures en werkprocessen voldoende is voor de risico's die worden gelopen bij het houden van de persoonsgegevens

Voor leden van SURF bestaat de mogelijkheid om ter invulling van de hierboven bedoelde audit deel te nemen aan SURFaudit. In dat geval is de gewenste uitkomst niveau 3 van het in de SURFaudit gebruikte Capability Maturity Model voor de normen die worden gesteld in het cluster 'toegangsbeveiliging'. Zie voor de SURFaudit: https://www.surf.nl/diensten-en-producten/surfaudit/index.html.

De Service Provider
SURFmarket en SURFnet besteden in afspraken met Service Providers aandacht aan beveiliging van (persoons)gegevens. Veel afspraken over beveiliging en/van (persoons)gegevens zijn het best op zijn plek in Verwerkersovereenkomsten die een Instelling zelf afsluit met een Service Provider.

SURFnet

Het beveiligingsbeleid van de SURFnet dienstverlening is gedocumenteerd. Het platform dat wordt ingezet voor de SURFconext-dienst wordt eens per twee jaar aan verschillende soorten audits onderworpen:

1. technische security audit; en
2. audit op de beheerprocessen.

De uitkomsten van audits zullen worden gedeeld met de Instellingen en eventueel met andere Identity Providers en Attribute Providers.

De virtuele toegang tot servers waarop het platform draait is beperkt met behulp van het SSH netwerk protocol. Serverruimten en serverkasten zijn op alle locaties afgesloten. De toegang tot fysieke ruimten wordt in logfiles vastgelegd en is alleen mogelijk voor daartoe geautoriseerde personen.

Indien er zich ten aanzien van de SURFnet dienstverlening beveiligingsincidenten voordoen, dan zal SURFnet deze vastleggen, analyseren en zo spoedig mogelijk rapporteren, inclusief geschatte impact, aan betrokken partijen.

SURFnet en Service Provider

Indien de Service Provider of SURFnet bij haar dienstverlening onderaannemers inschakelt zullen zij met de onderaannemer een overeenkomst aangaan waarin privacy bepalingen en geheimhoudings- en beveiligingsverplichtingen zijn opgenomen.

3.8 Wat zijn de bewaartermijnen en wanneer worden de gegevens verwijderd?

De algemene regel is dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waarvoor de gegevens zijn verzameld

SURFnet

SURFnet zal alle data over Gebruikers van de Instelling of overige Identity Providers/Attribute Providers, die binnen SURFconext aanwezig is, op verzoek van de Gebruiker verwijderen of anders automatisch 37 maanden na laatste inlog.

De persoonsgegevens in de logfiles van SURFnet worden uiterlijk 6 maanden bewaard.

De Service Provider

Afspraken over bewaartermijn van gegevens bij Service Providers legt de Instelling zelf vast in contracten met die Service Providers.