

Privacy Best Practice SURFfederatie

Inleiding

Om ervoor te zorgen dat de bij SURFnet aangesloten instellingen optimaal kunnen samenwerken met elkaar en met informatie- en dienstenleveranciers, heeft SURFnet de *SURFfederatie* opgezet. De SURFfederatie is een dienst waarbij een gebruiker, een student of medewerker van een instelling uit de doelgroep van SURFnet, met de elektronische identiteit die is verkregen bij de eigen instelling toegang kan krijgen tot diensten bij andere instellingen, of bij externe dienstenaanbieders, zoals uitgevers.

De dienst bestaat uit een set van afspraken, federatie-policy genoemd, en een technische infrastructuur. De technische infrastructuur bestaat uit een aantal door SURFnet centraal aangeboden voorzieningen waar instellingen en dienstenaanbieders aan kunnen koppelen. Deze voorzieningen vormen een centraal knooppunt waarlangs alle inlogverzoeken worden afgehandeld en de juiste kant op worden gestuurd. Zo hoeft een onderwijsinstelling niet zelf met alle dienstenaanbieders te koppelen, maar volstaat één koppeling met de SURFfederatie. Dezelfde constructie geldt uiteraard voor een dienstenaanbieder.

In de federatie-policy is ondermeer vastgelegd dat leden en partners van de SURFfederatie conform een privacy Best Practice zullen omgaan met persoonsgegevens binnen de SURFfederatie. Dit document beschrijft de privacy Best Practice. In deze Best Practice wordt het doel bepaald waarvoor persoonsgegevens worden verzameld en het gebruik beperkt voor zover dat noodzakelijk is voor het bereiken van een specifiek doel. Daarnaast wordt de toegang tot de persoonsgegevens beperkt tot degenen waarvoor toegang noodzakelijk is in het kader van het hierboven genoemde doel. De transparantie voor de gebruiker voor wat betreft de omgang met zijn persoonsgegevens wordt gewaarborgd door informatie te verstrekken aan de gebruiker zodra hij een dienst benadert via de federatie. Daarnaast zijn bewaartermijnen voor persoonsgegevens vastgesteld en worden federatiepartners en leden verplicht tot het nemen van beveiligingsmaatregelen om misbruik van de gegevens te voorkomen.

De privacy Best Practice is gebaseerd op de Wet Bescherming Persoonsgegevens (WBP). Voor wat betreft de onderwerpen die de Best Practice expliciet benoemt, is aansluiting gezocht bij de zogenaamde Vrijstellingsbesluiten bij deze wet. Uitgebreide toelichting op de WBP is te vinden op de site van het College Bescherming Persoonsgegevens: <http://www.cbppweb.nl/>

De privacy Best Practice wordt beschreven voor federatieleden en voor federatiepartners. Federatieleden zijn instellingen binnen de SURFnet doelgroep die willen aansluiten als verstrekker van identiteitsgegevens, ofwel *Identity Provider*, en/of als dienstenaanbieder, ofwel *Service Provider*.

Federatiepartners zijn organisaties buiten de doelgroep die zijn aangesloten op de SURFfederatie omdat zij voor de doelgroep interessante diensten leveren. Zij zijn dus per definitie een *Service Provider*.

In de rest van dit document zullen we steeds over de Identity- en de Service Provider spreken. Daarnaast gebruiken we de term SURFfederatie operator voor SURFnet, de beheerder van de centraal aangeboden voorzieningen en van de federatie-policy.

Als toelichting is in een bijlage van deze Best Practice een omschrijving van de SURFfederatie opgenomen waarbij duidelijk wordt op welke wijze en op welke momenten persoonsgegevens worden uitgewisseld bij het gebruik van de SURFfederatie.

Deze Best Practice zal initieel en na aanpassingen worden vastgesteld in de klankbordgroep van de SURFfederatie.

Privacy-bepalingen

Wat is doel van de gegevens-verwerking?

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 zal duidelijk zijn dat het doel vooraf moet worden geformuleerd. De wet 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

De Identity Provider beschikt los van het gebruik van de SURFfederatie over een basisadministratie van gebruikersgegevens. De gegevens afkomstig uit deze administratie zullen worden gebruikt om gebruikers toegang te verlenen tot diensten binnen de eigen instelling en tot het dienstenaanbod binnen de federatie. In het kader van het gebruik van de federatie kunnen nog extra gegevens van gebruikers worden verzameld indien dat voor toegang tot een bepaalde dienst noodzakelijk is.

De doelstelling van de basisadministratie is door de Identity Provider al voorafgaand aan de deelname aan de federatie vastgelegd. De doelstelling moet een verstrekking in het kader van de federatie niet in de weg staan en daarnaast moet het toevoegen van de gegevens specifiek voor de federatie passen binnen deze doelstelling. Een (deel) doelstelling van het bestand zou moeten luiden het verzamelen en verstrekken van gegevens in het kader van het verstrekken of ter beschikking stellen van diensten aan gebruiker op diens verzoek.

De Service Provider

De Service Provider verkrijgt gegevens van de Identity Provider ten behoeve van de authenticatie (het bewijs van authenticatie door de Identity Provider) en autorisatie van een gebruiker die toegang wil verkrijgen tot de door de Service Provider verleende dienst. Dit bestand met deze gegevens wordt in deze Best Practice het federatie-bestand genoemd (zie tekening in bijlage).

In het kader van deze Best Practice mag de Service Provider de gegevens die van de Identity Provider worden verkregen uitsluitend opslaan ten behoeve van het authenticeren en autoriseren voor de

diensten die de Service Provider biedt, communicatie over de services die de gebruiker afneemt en eventuele facturering van het gebruik.

De federatie-operator

SURFnet biedt de federatieleden en -partners de SURFfederatiedienst en treedt daarmee op als federatie-operator. Tijdens het federatieproces ontvangt de SURFfederatie operator persoonsgegevens van Identity Providers en stuurt deze door naar de Service Providers. In dit proces is de SURFfederatie operator niet meer dan een doorgeefluik, het is in feite de Identity Provider die gegevens verstrekt aan de Service Provider. Tijdens het proces slaat de SURFfederatie operator wel de gegevens op in een transactie- en authenticatielog. Ook worden tijdelijk persoonsgegevens vastgelegd in het kader van het ticketproces. Voor zover er geen gebruik wordt gemaakt van 'single sign on' zal de opslag van deze gegevens erg kort zijn (gedurende een sessie).

De doelstelling voor het verwerken van de persoonsgegevens is voor de federatie-operator beperkt tot het beheer en het uitvoeren van de federatiedienst (zie een iets uitgebreidere omschrijving hieronder bij logfiles)

Logfiles

Alle deelnemers aan de federatie zullen 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. Deze doelstelling brengt ook met zich mee dat de gegevens in de logfiles slechts voor een beperkte termijn zullen worden bewaard.

Welke gegevens worden vastgelegd?

In de privacywetgeving wordt aan het verzamelen van gegevens de eis gesteld dat er niet te veel of te 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).

Deelnemers aan de federatie zullen zich bij het verwerken van persoonsgegevens steeds de vraag moeten stellen of er niet met minder gegevens hetzelfde doel bereikt kan worden.

De gegevens moeten juist en nauwkeurig zijn. Dat betekent dat er periodieke 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. Daarom kent de wet voor deze gegevens een strenger regime, waarbij het uitgangspunt is dat deze zogenaamde 'bijzondere' gegevens niet mogen worden verwerkt. Uiteraard kent de wet een aantal specifieke uitzonderingen voor dit verbod. Voor de federatie geldt dat er door alle deelnemers geen bijzondere gegevens zullen worden verwerkt. Een overzicht van de bijzondere gegevens is opgenomen in een bijlage bij deze Best Practice.

Voor de Identity Provider

De gegevens die relevant zijn in het kader van de federatie zullen grotendeels al zijn opgenomen in de administratie van de Identity Provider. In het kader van de federatie mag de Identity Provider de volgende gegevens verwerken (voor zover al niet opgenomen)

- Gegevens voor identificatie van gebruikers (de userid, waarbij ook de instelling van de gebruiker is opgenomen).

Indien nodig voor het afnemen van de aangeboden dienst waartoe de gebruiker via de federatie toegang tot wil hebben kunnen ook de volgende persoonsgegevens opgenomen:

- 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 de federatie (denk aan studierichting, faculteit, functie, etc.).

Voor de Service Provider

De Service Provider zal de (categorieën van) gegevens zoals verstrekt door de Identity Provider verwerken en eventueel opslaan.

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.).

Voor de federatie-operator

De operator slaat uitsluitend transactie- en sessiegegevens op in haar logfiles.

Aan wie worden de gegevens verstrekt?

Voor de Identity Provider

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

Voor de Service Provider

Alleen met expliciete ondubbelzinnige toestemming van de gebruikers worden de persoonsgegevens uit het zogenaamde federatiebestand verstrekt aan derden. Alleen de gebruiker heeft toegang tot eventuele gebruikersprofielen voor zover deze niet geanonimiseerd zijn.

Voor de federatie-operator

De SURFfederatie operator draagt er zorg voor dat alleen degenen die belast zijn met beheerwerkzaamheden toegang hebben tot de gegevens in de logfiles. Verstrekkingen aan anderen in het geval van het behandelen van geschillen gebeurt alleen indien:

- Er ondubbelzinnig toestemming is verleend door de gebruiker.
- Het noodzakelijk is voor de nakoming van een wettelijke plicht van de SURFfederatie operator.

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

Logfiles

Hetgeen hierboven is opgenomen voor de logfiles van de federatie-operator geldt tevens voor de logfiles van de deelnemers in de federatie; de Service Providers en Identity Providers

Hoe wordt transparantie voor de gebruiker bewerkstelligd?

Een belangrijke doelstelling van de WBP 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 WBP legt ter bevorderingen van deze transparantie een aantal plichten bij de verantwoordelijke en een aantal rechten bij de betrokkenen. De deelnemers van de federatie dragen er zorg voor dat de gebruikers hun recht op inzage en correctie kunnen uitoefenen. De deelnemers hebben daarnaast een reglement voor de omgang met persoonsgegevens binnen hun organisatie en zorgen ervoor dat de gebruiker toegang heeft tot dit reglement.

Voor de Identity Provider

Op het beginscherm is een kennisgeving opgenomen dat de Identity Provider de gegevens uitsluitend verstrekt ten behoeve van de toegang tot de door gebruiker gewenste dienst. Het beginscherm is de webpagina waar de gebruiker moet aangeven welke instelling haar/zijn Identity Provider is. Merk op dat het beginscherm niet door de Identity Provider wordt gefaciliteerd, maar door de Service Provider of de SURFfederatie operator. De gevoerde tekst op dit scherm maakt deel uit van deze Best Practice en is als bijlage toegevoegd.

Voor 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.

Voor de federatie-operator

De SURFfederatie operator verkrijgt de gegevens van de gebruiker buiten hem/haar om. De gebruiker is zich er niet van bewust dat de SURFfederatie operator zijn gegevens verkrijgt. Op het beginscherm van de SURFfederatie operator of van de Service Provider is de kennisgeving opgenomen dat de SURFfederatie operator logfiles bijhoudt over het gebruik van de federatie. De kennisgeving verwijst tevens naar een webpagina bij de SURFfederatie operator waar haar contactgegevens te vinden zijn.

Hoe worden de persoonsgegevens beveiligd?

In de wet 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 in de federatie dragen zorg voor een adequate beveiliging tegen verlies, beschadiging en ongeoorloofde kennisneming of aanpassing van de gegevens.

Met adequaat wordt binnen de federatie bedoeld dat:

- Het beveiligingsbeleid van de deelnemers een uitspraak doet over de mate van beveiliging voor gegevens die te maken hebben met de transacties tussen de deelnemer en de federatie.
- Een classificatie en risicoanalyse hebben plaatsgevonden op de koppeling met de federatie.
- Door middel van een reguliere audit op de beveiliging wordt vastgesteld of deze op de punten techniek, procedures en werkprocessen voldoende is voor de risico's die worden gelopen bij het houden van het algemeen bestand en de logfiles.

Wat is de bewaartermijn van de gegevens ?

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

Voor de Identity Provider

Voor een personeelsregistratie geldt in z'n algemeenheid dat persoonsgegevens uiterlijk 2 jaar nadat het dienstverband of de werkzaamheden zijn beëindigd worden verwijderd. Voor de studentenadministratie geldt dat persoonsgegevens uiterlijk 2 jaar nadat de studie is beëindigd worden verwijderd.

Voor de Service Provider

De persoonsgegevens in het federatiebestand worden uiterlijk 2 jaar na de laatste transactie van de gebruiker bewaard.

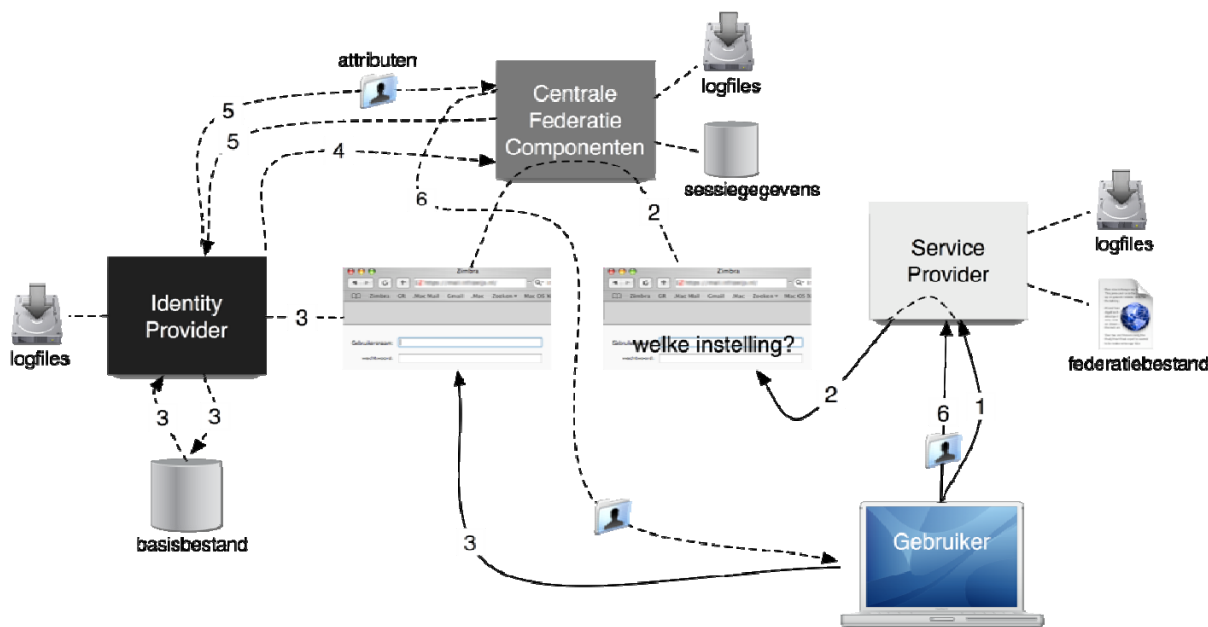
Voor de federatie-operator

De persoonsgegevens in de logfiles van de federatie-operator worden uiterlijk 6 maanden bewaard. Deze termijn geldt ook voor de logfiles van de Identity Providers en Service Providers van de federatie.

Bijlage 1: omschrijving SURFfederatie

De werking van de SURFfederatie wordt beschreven aan de hand van een scenario waarin een gebruiker van een instelling binnen de doelgroep wil inloggen op de website van een Service Provider. Uiteraard gaan we er van uit dat de betreffende instelling is aangesloten op de SURFfederatie en daarmee als Identity Provider fungeert.

De SURFfederatie bestaat uit een aantal centraal aangeboden voorzieningen. Deze worden de Centrale Federatie Componenten, of kortweg CFC, genoemd, die door de SURFfederatie operator (SURFnet) worden beheerd. In de onderstaande figuur zijn de CFC aangegeven in een schematisch overzicht van de SURFfederatie samen met een weergave van de gegevens die op de verschillende plaatsen in de federatie beschikbaar zijn.



De gestippelde lijnen in de figuur zijn voor de gebruiker onzichtbaar.

1. Een gebruiker komt bij een Service Provider en moet inloggen om gebruik te maken van diensten van de Service Provider. Uitgangspunten zijn dat de Service Provider niet tevens de instelling waar de gebruiker aan is verbonden (die mogelijkheid bestaat ook, maar is als voorbeeld minder interessant) en dat de Service Provider voor de toegang tot de betreffende diensten via de SURFfederatie aanbiedt.
2. De gebruiker wordt door de Service Provider doorgestuurd naar een webpagina (beginscherm) om bekend te maken bij welke instelling zij/hij hoort, of meer precies welke instelling haar/zijn Identity Provider is (Identity Provider discovery). Deze pagina kan door de Service Provider worden getoond of deel uitmaken van de CFC. Er zijn dus twee alternatieven, die in de figuur niet zijn onderscheiden. In beide gevallen spelen de CFC een rol.

a. De pagina is deel van de CFC

Zodra de gebruiker aangeeft te willen inloggen (bijvoorbeeld door op een inlogknop te klikken) wordt deze door de Service Provider doorgestuurd naar de CFC. Hier wordt gevraagd bij welke instelling de gebruiker hoort (Identity Provider selectie), waarna de gebruiker naar een webpagina van de betreffende Identity Provider wordt doorgestuurd om in te loggen.

b. De pagina wordt door de Service Provider aangeboden

Aan de gebruiker wordt gevraagd bij welke instelling deze hoort. Zodra deze dat heeft opgegeven wordt een authenticatieverzoek aan de CFC gestuurd door de dienstenaanbieder. De CFC geeft dit meteen door aan de Identity Provider. De gebruiker merkt dit niet en komt rechtstreeks op de inlogpagina van de Identity Provider terecht.

Een reden voor de Service Provider om zelf de zgn. "Identity Provider discovery" pagina aan te bieden kan zijn dat het dan in de eigen huisstijl kan worden getoond. Overigens geldt hierbij wel dat bepaalde teksten dienen te worden opgenomen die aan de gebruiker duidelijk maken wat er met haar/zijn identiteitsgegevens gebeurt binnen de federatie (zie de Best Practice voor de Service Provider).

3. Bij de authenticatiepagina van de Identity Provider aangekomen kan de gebruiker een userid en een wachtwoord invullen of zich op een andere manier authenticeren.
4. De gebruiker wordt door de Identity Provider weer teruggestuurd naar de CFC.
5. De CFC stelt vast dat bij de Identity Provider authenticatie heeft plaatsgevonden. Als het antwoord positief is worden de gewenste attributen, bestaande uit een *userid* en eventuele verdere gegevens (attributen), die de Identity Provider aan de Service Provider wil vrijgeven, bepaald. Dit gebeurt voor de gebruiker op de achtergrond.
6. De CFC stuurt de gebruiker door naar de Service Provider. Deze stelt vast dat de gebruiker via de CFC is geauthenticeerd waarna de gebruiker de gewenste diensten kan gaan gebruiken. Hierbij worden tevens alle attributen uit stap 5 doorgestuurd. Merk op dat de stappen 4 en 5 voor de gebruiker onzichtbaar zijn.

Hierbij dienen enkele kanttekeningen gemaakt te worden.

- Indien bij stap 3 bleek dat het resultaat van de authenticatie negatief was, dan krijgt de gebruiker dit op het scherm van de Identity Provider te zien en komt dan niet meer automatisch terug bij de dienstenaanbieder.
- De vorm van de userid wordt door de identiteitsverstrekker bepaald en daarmee is de gebruiker dus identificeerbaar. Het mechanisme blijft echter werken als de identiteitsverstrekker de userid-op de naam van de instelling na - anonimiseert voor de buitenwereld.
- De extra attributen die worden meegestuurd zijn vastgelegd in een *richtlijn*, die de Identity Provider heeft ten aanzien van elke dienstenaanbieder. Deze richtlijn kan door de Identity Provider ook nog worden gedifferentieerd per gebruiker of gebruikersgroep. In de praktijk is zo'n differentiatie echter beheerintensief.

- Als de Service Provider meer attributen wil dan een richtlijn toestaat, dan zal deze die attributen zelf aan de gebruiker moeten vragen. Dat kan direct na stap 6 gebeuren. De gebruiker zou dan zelf extra gegevens kunnen invullen (of besluiten om dat niet te doen).
- Om het doorsturen goed te laten verlopen wordt bij een inlogsessie gebruik gemaakt van tickets. De CFC houden in een database *sessiegegevens* bij, die bestaan uit een ticket met alle attributen, inclusief de userid. Dit ticket wordt in principe zeer kort, gedurende het inloggen (enkele minuten) vastgehouden. De periode wordt in de CFC ingesteld en moet lang genoeg zijn om de stappen 3,4 en 5 te overbruggen.
- Indien single sign on wordt aangeboden door de SURFfederatie, hoeft de gebruiker gedurende een langere periode niet opnieuw in te loggen voor meerdere diensten waarvoor de authenticatie via de SURFfederatie verloopt. In dit geval wordt het ticket door de CFC gedurende die periode bewaard en op de achtergrond gebruikt voor nieuwe authenticatieverzoeken. Indien extra attributen nodig zijn voor nieuwe diensten worden deze ook zonder nieuwe authenticatie door de gebruiker opgevraagd bij de Identity Provider en verstrekt aan de dienstenaanbieder. Single sign on wordt op dit moment niet geboden.
- Er worden door de Identity Provider, de Service Provider en de SURFfederatie operator een transactielog en een authenticatielog bijgehouden. Hierin staan de userid's van de gebruikers vermeld.
- Een Service Provider houdt eventueel een *federatiebestand* bij ten behoeve van
 - het valideren van authenticatiegegevens en autoriseren voor de services die de Service Provider biedt;
 - communicatie over de services die de gebruiker afneemt;
 - eventuele facturering over het gebruik.

Bijlage 2: Tekst beginscherm

Privacy-verklaring SURFfederatie

De SURFfederatie hecht veel belang aan de privacy van gebruikers. Voor de omgang met persoonsgegevens is binnen de SURFfederatie een Privacy Best Practice opgesteld. Deze Best Practice is te vinden op <https://federatie.surfnet.nl>

Persoonsgegevens zullen in het kader van de federatie alleen worden verstrekt indien dat noodzakelijk is voor de authenticatie en autorisatie van de gebruiker die toegang zoekt tot een dienst. Service Providers zullen de gegevens alleen opslaan voor het authenticeren en autoriseren en indien van toepassing voor het communiceren met de gebruiker over de verleende dienst en eventuele facturering van het gebruik. De Service Provider verstrekt geen gegevens aan derden.

Tot de gegevens in logfiles van een Service Provider en bij de SURFfederatie hebben alleen degene toegang die belast zijn met beheer. Deze gegevens worden niet verstrekt en kennen een maximale bewaartermijn van een half jaar.

De gebruiker kan met vragen over de omgang van zijn of haar persoonsgegevens binnen de federatie terecht bij de eigen instelling of de Service Provider bij wie de gebruiker een dienst heeft afgenomen. Een overzicht van deelnemende instellingen en Service Providers is te vinden op <http://federatie.surfnet.nl>

Bijlage 3: bijzondere gegevens

Bijzondere persoonsgegevens zijn alle persoonsgegevens die informatie verschaffen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging. Verder zijn strafrechtelijke persoonsgegevens in ruime zin (niet alleen veroordelingen, maar ook verdenkingen of bijvoorbeeld een straatverbod) bijzondere gegevens.