SURFnet Verwerkersovereenkomst

inzake gebruik SURFnet diensten

tussen

en

SURFnet bv

9 november 2018

Versienummer 1.0, Verwerkersovereenkomst SURFnet diensten d.d. 9 november 2018.

Partijen

Organisatie, gevestigd aan te en rechtsgeldig vertegenwoordigd door (hierna: **"Verwerkingsverantwoordelijke"**);

SURFnet, gevestigd aan het Moreelsepark 48 te Utrecht, Kamer van Koophandel nummer 30090777 en rechtsgeldig vertegenwoordigd door (hierna: "Verwerker");

Hierna gezamenlijk te noemen: "**Partijen**" en individueel te noemen "**Partij**";

in aanmerking nemende dat:

- Partijen hebben op een Gebruiksovereenkomst gesloten met kenmerk / (hierna: "de Overeenkomst") met betrekking tot de dienstverlening van SURFnet. Ter uitvoering van de Gebruiksovereenkomst verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens;

- In het kader van het uitvoeren van de Overeenkomst is SURFnet aan te merken als Verwerker in de zin van de AVG en is Organisatie aan te merken als Verwerkingsverantwoordelijke in de zin van de AVG;

- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;

- Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

- Partijen maken onderdeel uit van de SURF coöperatie. In de SURF coöperatie werken Partijen samen aan een optimale inzet van informatie- en communicatietechnologie ten behoeve van onderwijs en onderzoek. De dienstverlening binnen de coöperatie vindt plaats binnen de werkmaatschappijen: SURFnet, SURFmarket en SURFsara. Hierna gezamenlijk te noemen: "SURF werkmaatschappijen".

- De SURF werkmaatschappijen hebben bij het opstellen van deze Verwerkersovereenkomst voor de dienstverlening van de betreffende werkmaatschappij de binnen de SURF coöperatie opgestelde SURF model verwerkersovereenkomst (versie oktober 2017) als uitgangspunt genomen.

- De SURF werkmaatschappijen hebben hun dienstverlening zoveel mogelijk in lijn gebracht met de verplichtingen uit deze Verwerkersovereenkomst waarbij de concrete invulling vanwege de aard van de dienstverlening of inrichting van de betreffende werkmaatschappij kan verschillen.

- Voor zover SURFnet een Dienst (nog) niet volledig kan voldoen aan de verplichtingen uit deze Verwerkersovereenkomst, wordt dit beschreven in de dienst-specifieke Bijlage A.

- De SURF model Verwerkersovereenkomst geeft een keuzemogelijkheid met betrekking tot het geven van specifieke of algemene toestemming voor het inschakelen van Sub-verwerkers. In deze Verwerkersovereenkomst geeft Verwerkingsverantwoordelijke algemene toestemming voor het inschakelen van Sub-verwerkers door Verwerker.

- In deze Verwerkersovereenkomst is in de artikelen 5.4; 5.9; 7.5; 12.2 en 14.2 opgenomen dat Partijen in overleg c.q. onderhandeling (kunnen) treden. Ook indien met het verlenen van bijstand door Verwerker substantiële kosten gemoeid zijn die redelijkerwijs niet uitsluitend bij Verwerker kunnen worden neergelegd, treden Partijen in overleg over de verdeling van kosten.

- Meer algemeen staan Partijen open voor overleg indien over de toepassing of betekenis van bepalingen van deze Verwerkersovereenkomst onduidelijkheid bestaat of een verschil van mening optreedt tussen Partijen. Partijen zullen bij het overleg over toepassing en/of betekenis steeds uitgaan van de onderlinge samenwerking en de gemeenschappelijke belangen binnen de SURF coöperatie.

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

1.1. **AVG**: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.2. **Betrokkene**: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

1.3. **Bijlage**: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.4. **Bijzondere categorieën Persoonsgegevens**: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

1.5. **Derde**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

1.6. **Dienst**: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Verwerkingsverantwoordelijke.

1.7. **Inbreuk in verband met Persoonsgegevens**: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8. **Medewerker**: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9. **Ontvanger**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10. **Overeenkomst**: de (Gebruiks)overeenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

1.11. **Persoonsgegeven**: alle informatie over een Betrokkene; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12. **PIA**: de gegevensbeschermingseffectbeoordeling (privacy impact assessment) die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.13. **Schriftelijk**: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.14. **Sub-verwerker**: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

1.15. **Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens**: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16. **Toezichthoudende autoriteit**: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

1.17. **Verwerkersovereenkomst**: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

1.18. **Verwerking**: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 onder 2) AVG.

ARTIKEL 2. VOORWERP VAN DE VERWERKERSOVEREENKOMST

2.1. De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens. Bij tegenstrijdigheid tussen de bepalingen uit de Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

2.2. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

2.3. Verwerkingsverantwoordelijke geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke. De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4. Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamedoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.5. Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker een instructie

van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

2.6. Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd.

ARTIKEL 3. VERWERKING VAN PERSOONSGEGEVENS

3.1. Voorafgaand aan het sluiten van de Verwerkersovereenkomst informeert Verwerker Verwerkingsverantwoordelijke in Bijlage A volledig en naar waarheid over de Verwerkingen die Verwerker ter uitvoering van de Overeenkomst uitvoert, tenzij in Bijlage A is opgenomen dat Verwerkingsverantwoordelijke de betreffende informatie in deze Bijlage opneemt. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

ARTIKEL 4. VERLENEN VAN BIJSTAND EN MEDEWERKING

4.1. Verwerker verleent Verwerkingsverantwoordelijke alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. Verwerker verleent Verwerkingsverantwoordelijke in ieder geval bijstand met betrekking tot:

(i) De beveiliging van Persoonsgegevens;

(ii) Het uitvoeren van controles en audits;

(iii) Het uitvoeren van PIA's;

(iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;

(v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;

(vi) Het voldoen aan verzoeken van Betrokkenen;

(vii) Het melden van Inbreuken in verband met Persoonsgegevens.

4.2. Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.1. Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

4.3.2. Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Verwerkingsverantwoordelijke – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Verwerkingsverantwoordelijke met een verzoek om nadere instructies.

4.3.3. Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

4.3. Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.4. Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Verwerkingsverantwoordelijke onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van Verwerkingsverantwoordelijke in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Verwerkingsverantwoordelijke.

4.3.5. Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

4.3.2.1. Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Verwerkingsverantwoordelijke op grond van artikel 4.3.1 te voldoen.

4.3.2.2. Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of de instructies van Verwerkingsverantwoordelijke op te volgen.

4.3.2.3. Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

4.3.2.4. Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

ARTIKEL 5. TOEGANG TOT PERSOONSGEGEVENS

5.1. Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Sub-verwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

5.2. Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is. De categorieën Medewerkers zijn in Bijlage A gespecificeerd.

5.3. Verwerkingsverantwoordelijke verschaft met het aangaan van deze overeenkomst algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers door Verwerker. Voor het inschakelen van de in Bijlage A opgenomen Sub-verwerkers wordt met het tekenen van deze Verwerkersovereenkomst toestemming gegeven.

5.4. Verwerker licht Verwerkingsverantwoordelijke uiterlijk drie (3) maanden voorafgaand aan beoogde veranderingen inzake de toevoeging, vervanging of wijziging van Sub-verwerker(s), Schriftelijk in, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Partijen treden hierop in onderhandeling.

5.5. De algemene toestemming van Verwerkingsverantwoordelijke voor het inschakelen Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 9, onverlet. Verwerkingsverantwoordelijke kan zijn algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers intrekken, indien Verwerker niet of niet langer voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

5.6. Verwerker verstrekt op eerste verzoek van Verwerkingsverantwoordelijke een overzicht van de door Verwerker ingeschakelde Sub-verwerkers aan Verwerkingsverantwoordelijke.

5.7. Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.

5.8. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9. Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Indien geheimhouding of andere contractuele afspraken met Sub-verwerker het delen van een afschrift van de Schriftelijke overeenkomst in de weg staat, treedt Verwerker in overleg met Sub-verwerker om zo goed mogelijk in de informatieverstrekking aan Verwerkingsverantwoordelijke te (kunnen) voorzien.

5.10. Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, voortvloeiende uit de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

ARTIKEL 6. BEVEILIGING

6.1. Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

6.2. Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.3. Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker inzage in het beveiligingsbeleid van Verwerker.

6.4. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

ARTIKEL 7. AUDIT

7.1. Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet. Bovenstaande verplichting zal door Verwerker worden ingevuld door dienst specifieke systemen en/of processen en/of (beveiligings-)maatregelen te laten auditen door een externe partij. De inhoud, omvang en planning is opgenomen in het auditprogramma per dienst in Bijlage B.

7.2. Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1. Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3. Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage B is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

7.4. Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Verwerkingsverantwoordelijke verricht. Indien Verwerker niet beschikt over een verklaring zullen de bevindingen van de audit met Verwerkingsverantwoordelijke worden gedeeld.

7.5. Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet. Bij een audit op verzoek van Verwerkingsverantwoordelijke zullen Verwerker en Verwerkingsverantwoordelijke in overleg tot overeenstemming komen over de termijn waarop de audit plaatsvindt. Gedurende de audit op verzoek respecteert Verwerkingsverantwoordelijke het beveiligingsbeleid en de bedrijfsactiviteiten van de Verwerker.

7.6. De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de

bepalingen uit de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

7.7. Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

ARTIKEL 8. INBREUK IN VERBAND MET PERSOONSGEGEVENS

8.1. Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersoon en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van hetgeen is opgenomen in Bijlage C. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

8.2. Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit Bijlage C gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

8.3. Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Verwerkingsverantwoordelijke hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

8.4. Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker Verwerkingsverantwoordelijke een afschrift van dit register.

ARTIKEL 9. DOORGIFTE VAN PERSOONSGEGEVENS

9.1. Persoonsgegevens mogen enkel worden doorgegeven aan derde landen of internationale organisaties indien sprake is van een passend beschermingsniveau en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze

bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

9.2. Verwerkingsverantwoordelijke kan aan de Schriftelijke toestemming, zoals bedoeld in artikel 9.1, nadere voorwaarden verbinden, waaronder maar niet beperkt tot het aantonen dat aan de vereisten zoals opgenomen in artikel 9.3 is voldaan.

9.3. Verwerkingsverantwoordelijke kan Verwerker slechts toestemming verlenen voor een doorgifte van Persoonsgegevens aan derde landen of internationale organisaties indien, ofwel:

(i) Een adequaatheidsbesluit overeenkomstig artikel 45 lid 3 AVG is genomen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(ii) Passende waarborgen overeenkomstig artikel 46 AVG met inbegrip van bindende voorschriften zoals bedoeld in artikel 47 AVG, zijn getroffen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(iii) Aan één van de specifieke voorwaarden uit artikel 49 lid 1 AVG is voldaan ten aanzien van het betreffende derde land of de betreffende internationale organisatie.

ARTIKEL 10. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

10.1. Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

10.2. Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

(i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;

(ii) Enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partij hiervan op de hoogte stellen;

(iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partij.

10.3. Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

ARTIKEL 11. AANSPRAKELIJKHEID EN VRIJWARING

11.1. Verwerker is aansprakelijk voor de schade die voortvloeit uit of verband houdt met het niet nakomen van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

11.2. Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken, boeten en/of maatregelen van derden, daaronder begrepen Betrokkenen en de Toezichthoudende autoriteit, die jegens Verwerkingsverantwoordelijke worden ingesteld of opgelegd wegens een schending van de

Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens door Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers

11.3. De uit artikel 11.1 en 11.2 voortvloeiende aansprakelijkheid voor Verwerker is beperkt tot een bedrag van EURO 100.000,- per aanspraak. Samenhangende aanspraken worden daarbij aangemerkt als één aanspraak. Deze beperking van aansprakelijkheid komt te vervallen indien sprake is van opzet of grove schuld aan de zijde van de Verwerker.

11.4. Verwerker draagt zorg voor afdoende dekking van de aansprakelijkheid door middel van een aansprakelijkheidsverzekering. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker Verwerkingsverantwoordelijke inzage in (de polis van) deze aansprakelijkheidsverzekering van Verwerker

ARTIKEL 12. WIJZIGING

12.1. Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens. Hieronder wordt in ieder geval verstaan:

(i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;

(ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;

(iii) Het inschakelen van andere Sub-verwerkers;

(iv) Wijziging in de doorgifte van Persoonsgegevens aan derde landen en/of internationale organisaties.

12.2. Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Verwerkingsverantwoordelijke in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3. Verwerker is pas gerechtigd tot het uitvoeren van een wijziging in de Dienst, een wijziging in de uitvoering van de Overeenkomst, een wijziging in de uitvoering van de Verwerkersovereenkomst en/of een wijziging die aanpassing van Bijlage A tot gevolg heeft, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven. Onder een wijziging in de Dienst wordt verstaan een substantiële wijziging die gevolgen kan hebben voor de Verwerking van Persoonsgegevens. Verwerker kan zonder voorafgaande Schriftelijke toestemming van Verwerkingsverantwoordelijke direct noodzakelijke aanpassingen of wijzigingen uitvoeren, bijvoorbeeld met betrekking tot adequate beveiliging van de dienst. Verwerker zal Verwerkingsverantwoordelijke zo spoedig mogelijk informeren over de wijziging.

12.4. Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

12.5. In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

ARTIKEL 13. DUUR EN BEËINDIGING

13.1. De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Verwerkersovereenkomst van rechtswege en vice versa.

13.2. Verwerkingsverantwoordelijke is gerechtigd de Verwerkersovereenkomst op te zeggen, indien Verwerker niet voldoet of niet langer kan voldoen aan de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zonder dat Verwerker aanspraak maakt op enige schadevergoeding. Bij de opzegging neemt Verwerkingsverantwoordelijke een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke opzegging rechtvaardigen.

13.3. Binnen een maand nadat de Overeenkomst eindigt, vernietigt en/of retourneert Verwerker alle Persoonsgegevens en/of draagt Verwerker deze over aan Verwerkingsverantwoordelijke en/of een andere door Verwerkingsverantwoordelijke aan te wijzen partij, naar gelang de keuze van Verwerkingsverantwoordelijke. Alle bestaande (overige) kopieën van Persoonsgegevens, zich al dan niet bevindende bij door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, worden hierbij aantoonbaar permanent verwijderd, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

13.4. Verwerker bevestigt op verzoek van Verwerkingsverantwoordelijke Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 13.3 heeft voldaan.

13.5. Verwerker draagt de kosten voor vernietiging, retournering en/of overdracht van de Persoonsgegevens. Verwerkingsverantwoordelijke kan nadere eisen stellen aan de wijze van vernietiging, retournering en/of overdracht van de Persoonsgegevens, waaronder eisen aan het bestandsformaat. Bij de overdracht van Persoonsgegevens wordt uitgegaan van een open bestandsformaat.

13.6. Verplichtingen uit de Verwerkersovereenkomst die naar hun aard bestemd zijn om na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst voortduren.

ARTIKEL 14. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

14.1. De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2. Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar Verwerkingsverantwoordelijke gevestigd is. Alvorens het geschil voor te leggen aan de bevoegde rechter zullen Partijen zich inspannen om in onderling overleg tot een beslechting van het geschil te komen.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN:

Plaats:	Plaats: Utrecht
d.d. _____	d.d.
Organisatie	SURFnet bv

Naam:_____

Functie:_____

Bijlage A8: Specificatie van de Verwerking van Persoonsgegevens SURFconext

Datum versie: 9 november 2018

Omschrijving van de Verwerking
De opdracht is het door SURFnet aan instellingen leveren van de dienst SURFconext. SURFconext biedt instellingen de mogelijkheid om gebruikers met het instellingsaccount veilig in te laten inloggen bij (cloud)diensten. Gebruikers die gebruik willen maken van diensten die gekoppeld zijn aan SURFconext, loggen in bij de thuisinstelling en na een succesvolle authenticatie geeft SURFconext aan de dienst door dat de gebruiker succesvol heeft ingelogd (zogenaamde 'federatieve authenticatie'). Daarbij worden er gegevens die de instelling levert aan SURFnet, eventueel na filtering en bewerking, doorgegeven aan de dienstaanbieder.

Doeleinden van de Verwerking
Het verwerken van persoonsgegevens is noodzakelijk voor het bieden van de dienst SURFconext (en gerelateerde functionaliteit, zoals genoemd op https://www.surf.nl/diensten-en-producten/surfconext/wat-is-surfconext/index.html). De persoonsgegevens worden ook verwerkt voor het bieden van support m.b.t. SURFconext, het afleggen van verantwoording (wie heeft wanneer welke dienst geactiveerd, bijvoorbeeld) en probleemoplossing. Zie ook https://wiki.surfnet.nl/display/conextsupport/Privacy+Policy+SURFconext .

Categorieën Betrokkenen
De betrokkenen zijn gebruikers van de dienst SURFconext. Een gebruiker is een op enigerlei wijze aan instelling verbonden natuurlijke persoon, die door de instelling geautoriseerd is tot (een bepaald deel van) de dienst. Meer specifiek kunnen gebruikers zijn:
• een persoon met een aanstelling dan wel een arbeidsovereenkomst bij de instelling;
• een bij de Instelling ingeschreven student, extraneus of cursist;
• een persoon die anderszins in het kader van de taakuitvoering van de instelling geautoriseerd is;
• een persoon die behoort tot een groep die in overeenstemming tussen Instelling, Service Provider en SURFnet toegang is verleend tot SURFconext en gelieerd is aan onderwijs en onderzoek in Nederland.

(categorieën) Persoonsgegevens
Attributen SURFconext:
SURFconext ondersteunt, op verzoek van de instelling, het vrijgeven van een aantal attributen aan Service Providers. Een actuele lijst van de vrij te geven attributen is te vinden op: https://wiki.surfnet.nl/display/surfconextdev/Attributen+in+SURFconext . Op deze pagina staat ook welke persoonsgegevens waar van afkomstig zijn. Welke en hoeveel attributen worden verstrekt verschilt per Service Provider. Via https://dashboard.surfconext.nl is na te gaan welke attributen een Service Provider vraagt ten behoeve van de dienstverlening aan de betrokkene. Een actueel overzicht van Service Providers waarvan de instelling heeft aangegeven dat verstrekking van attributen gewenst is - inclusief de bijbehorende attributen – is steeds toegankelijk via https://dashboard.surfconext.nl.
Betrokkenen kunnen op https://profile.surfconext.nl/my-services per dienst zien sinds wanneer welke gegevens zijn doorgegeven.

Accountgegevens:
SURFconext kan (cloud)diensten een privacyvriendelijke identifier (nummer) geven waarmee een gebruiker herkend kan worden als deze opnieuw inlogt bij een dienst. Om dit te kunnen doen, moet SURFconext de gebruikers-ID en de naam van de instelling opslaan.

Voor elke gebruiker wordt opgeslagen welke diensten gebruikt zijn en wanneer er voor het eerst is ingelogd op de dienst. Ook wordt bijgehouden of de gebruiker (of de instelling) toestemming heeft gegeven voor de doorgifte van attributen.
Voor elke gebruiker wordt bijgehouden wanneer deze voor het laatst heeft ingelogd via SURFconext.

SURFconext Teams:
Met SURFconext Teams kunnen studenten, onderzoekers en medewerkers van instellingen samenwerkingsgroepen beheren. Het beheer van de groepen wordt centraal geregeld en de groepen kunnen gebruikt worden bij verschillende op SURFconext gekoppelde Service Providers.
Voor SURFconext Teams worden de attributen van SURFconext verwerkt en opgeslagen.

Support:
SURFnet levert support aan gebruikers van de dienst, in geval de gebruiker problemen ervaart met de dienst. Daarbij worden persoonsgegevens
van de gebruiker verwerkt, zoals naam en e-mailadres.
Deze Persoonsgegevens worden enkel verwerkt indien noodzakelijk voor het leveren van support en enkel op verzoek van de gebruiker. Het wissen van gegevens is mogelijk op verzoek van de instelling of op verzoek van de betrokkene.

Loggegevens, ten behoeve van beveiliging en beheer van de dienst.

Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen
De bewaartermijn voor accountgegevens en SURFconext Teams is zevenendertig maanden na laatste inlog. Loggegevens worden 6 maanden bewaard.
Het wissen van gegevens binnen SURFconext is verder mogelijk op verzoek van de instelling of op verzoek van de betrokkene.

Categorieën Medewerkers

Categorieën Medewerkers (functierollen/functiegroepen) van Verwerker die Persoonsgegevens Verwerken	**(categorie) Persoonsgegevens die door Medewerkers worden verwerkt**	**Soort Verwerking**	**Land van Verwerking**
Technisch Product Managers SURFconext	Persoonsgegevens met betrekking tot het gebruik van de dienst, ten behoeve van het beheer en ondersteuning, inclusief loggegevens	Verwijderen, kopiëren, lezen	Nederland
Product Managers SURFconext	Persoonsgegevens met betrekking tot het gebruik van de dienst, ten behoeve van het beheer en ondersteuning.	Lezen	Nederland
Support Team SURFconext	Persoonsgegevens met betrekking tot het gebruik van de dienst,	Lezen	Nederland

	ten behoeve van het beheer en ondersteuning.		
Beheerteam SURFnet virtualisatie platform (SVP), interne SURFnet dienst NB. het SVP maakt ook gebruik van sub-verwerkers (zie tabel sub-verwerkers)	Inzien van metadata, maar niet van inhoud VM's	Lezen, veranderen, verwijderen, vernietigen, kopiëren	Nederland

Sub-verwerkers

Sub-verwerker die door Verwerker wordt ingeschakeld voor het Verwerken van Persoonsgegevens	**(categorie) Persoonsgegevens die Sub-verwerker verwerkt**	**Soort Verwerking**	**Land van Verwerking**	**Vestigings-land Sub-verwerker**
Proxy Services B.V.	Technisch beheer van SURFconext. Persoonsgegevens van betrokkenen die we verkrijgen door gebruik van de dienst, ten behoeve van het beheer en ondersteuning, inclusief loggegevens	Technisch beheer. Verwijderen, kopiëren, lezen	Nederland	Nederland
Interxion, Nikhef, Universiteit van Tilburg en UMC Utrecht	Geen (enkel fysieke opslag)	Bieden housing ten aanzien van het SVP	Nederland	Nederland
Prolocation	Inzien van metadata maar niet van inhoud VM's	Beheer en hardware en virtualisatielaag van het SVP	Nederland	Nederland

Doorgiften

Beschrijving doorgifte
Aanvulling op artikel 9 van de verwerkersovereenkomst: Via SURFconext kunnen gebruikers diensten gebruiken die gegevens verwerken buiten de EER. Doorgifte buiten de EER vindt plaats op verzoek van de instelling: SURFnet verstrekt uitsluitend persoonsgegevens aan Service Providers gekoppeld aan de dienst, indien de instelling hiertoe middels het hiertoe ingericht dashboard heeft aangegeven dat doorgifte van de persoonsgegevens gewenst is, zodat gebruikers toegang verkrijgen tot de door Service Provider verleende diensten. Deze werkwijze geldt als specifieke schriftelijke toestemming zoals beschreven in artikel 9.

Contactgegevens

Algemene contactgegevens	Naam	Functie	E-mail adres	Telefoonnummer
Verwerkings-verantwoordelijke		Instellingscontact-persoon (ICP)	Actueel e-mailadres wordt bijgehouden door klantsupport van SURFnet	Actueel telefoonnummer wordt bijgehouden door klantsupport van SURFnet
Verwerker	F.M. Morsch	Teamhoofd SURFconext	info@surfconext.nl	088 787 3000

Contactgegevens bij Inbreuk in verband met Persoonsgegevens	Naam	Functie	E-mail adres	Telefoonnummer
Verwerkings-verantwoordelijke		Instellingscontact-persoon (ICP) en indien opgegeven de contactpersoon 'Meldpunt datalekken SURFnet'	Actueel e-mailadres wordt bijgehouden door klantsupport van SURFnet	Actueel telefoonnummer wordt bijgehouden door klantsupport van SURFnet
Verwerker	SURFcert	Incident Response	cert@surfnet.nl	+31887873000

Afwijkingen en aanvullingen t.a.v. bepalingen verwerkersovereenkomst
N.v.t

Bijlage B: Beveiligingsmaatregelen

Versienummer 1.0, behorende bij Verwerkersovereenkomst SURFnet diensten d.d. 9 november 2018.

Deze Bijlage B is van toepassing voor alle door SURFnet geleverde diensten waarbij SURFnet optreedt als Verwerker.

Uitwerking van de door Verwerker getroffen beveiligingsmaatregelen:

SURFnet past het op ISO 27002 gebaseerde Normenkader Informatiebeveiliging Hoger Onderwijs toe bij de inrichting van de beveiliging van haar diensten. Met betrekking tot een adequate bescherming van persoonsgegevens gaat het steeds om maatregelen met betrekking tot de volgende onderwerpen:

- Inventory: er is een actueel en compleet overzicht van de voor de dienst gebruikte infrastructuur en middelen
- Rollen en verantwoordelijkheden: er is een actueel en compleet overzicht van rollen, taken en verantwoordelijkheden voor de dienst
- Wijzigingsbeheer: op een gecontroleerde wijze worden wijzigingen doorgevoerd inclusief besluitvorming, test- en fall back mechanismes etc.
- Vulnerability management/patching: de dienst kent mechanismen voor detectie, beheer en verhelpen van kwetsbaarheden
- Toegangsbeperking (logisch): er zijn mechanismen voor het verlenen van toegang, het controleren van rechten en het intrekken van de toegang
- Hardening/access control: maatregelen die toegang tot de systemen, infrastructuur en gegevens beperken en misbruik voorkomen (hardening van systemen, firewalls, ACLs etc., bescherming van opgeslagen gegeven en van gegevenstransport)
- Standaardisatie bij software ontwikkeling: er wordt gebruik van standaarden voor software ontwikkeling en mechanisme voor het controleren van de kwaliteit.
- Logging en monitoring: monitoring en logging vinden plaats waarbij omvang en doelstelling is vastgelegd.
- Incident respons: er zijn procedures opgesteld voor het melden, analyseren, verhelpen en rapporteren van security incidenten in de hele keten.
- Afspraken leveranciers: in contracten, SLA’s, DAPS etc. zijn de afspraken vastgelegd met leveranciers, inclusief rapportages en periodiek overleg
- Afspraken/screening met/van betrokken medewerkers: aan medewerkers, inhuur en medewerkers bij leveranciers worden eisen gesteld m.b.t. vertrouwelijkheid en integriteit.
- Auditprogramma: er is een auditprogramma voor de controle van de effectiviteit van de genomen beveiligingsmaatregelen.

De specifieke invulling van de beveiligingsmaatregelen voor de dienst kan worden opgevraagd bij de contactpersoon van de dienst zoals opgenomen in Bijlage A van de betreffende dienst.

Informatie over audit programma Verwerker

Bij SURFnet wordt de audit per product/dienst georganiseerd en uitgevoerd. Afhankelijk van de aard van de dienst worden de volgende audits uitgevoerd:

- Proces audits: audit op relevante beheerprocessen
- Technische audits: op delen van de infrastructuur waarbij type audit en diepgang kunnen variëren (bijvoorbeeld pentesten). De audit wordt regulier uitgevoerd maar ook naar aanleiding van grote infrastructuur wijzigingen, een grote storing of incident.
- Code review: indien voor het product software ontwikkeld is dan wordt een geheel of gedeeltelijk code review audit uitgevoerd.

Het betreft audits die door onafhankelijke, deskundige externe partijen uitgevoerd worden.

De persoonsgegevens die in de dienst worden verwerkt zijn zodanig geclassificeerd dat Verwerker tenminste een keer per twee jaar een audit verricht. Het audit programma voor de dienst - waar zowel al uitgevoerde als geplande audits zijn opgenomen - is uiterlijk 1 januari 2019 compleet en kan worden opgevraagd bij de contactpersoon zoals opgenomen in Bijlage A van de betreffende dienst.

Bijlage C: Informatie die moet worden verstrekt bij een Inbreuk in verband met Persoonsgegevens

Versienummer 1.0, behorende bij Verwerkersovereenkomst SURFnet diensten d.d. 9 november 2018.

Deze Bijlage C is van toepassing voor alle door SURFnet geleverde diensten waarbij SURFnet optreedt als Verwerker.

Contactgegevens melder

Naam, functie, emailadres, telefoonnummer.

Gegevens over de Inbreuk in verband met Persoonsgegevens (hierna: "Inbreuk")

- Geef een samenvatting van het incident waarbij de Inbreuk op de beveiliging van Persoonsgegevens zich heeft voorgedaan.
- Van hoeveel personen zijn Persoonsgegevens betrokken bij de Inbreuk?
  (Vul de aantallen in.)
  - a) Minimaal: (vul aan)
  - b) Maximaal: (vul aan)
- Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken (Categorieën Betrokkenen) bij de Inbreuk.
- Wanneer vond de Inbreuk plaats?
  (Kies een van de volgende opties en vul waar nodig aan)
  - a) Op (datum)
  - b) Tussen (begindatum periode) en (einddatum periode)
  - c) Nog niet bekend
- Wat is de aard van de Inbreuk?
  (U kunt meerdere mogelijkheden aankruisen)
  - a) Lezen (vertrouwelijkheid)
  - b) Kopiëren
  - c) Veranderen (integriteit)
  - d) Verwijderen of vernietigen (beschikbaarheid)
  - e) Diefstal
  - f) Nog niet bekend
- Om welk type Persoonsgegevens gaat het?
  (U kunt meerder mogelijkheden aankruisen)
  - a) Naam -, adres - en woonplaatsgegevens

b) Telefoonnummers

c) E - mailadressen of andere adressen voor elektronische communicatie

d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)

e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)

f) Burgerservicenummer (BSN) of sofinummer

g) Paspoortkopieën of kopieën van andere legitimatiebewijzen

h) Geslacht, geboortedatum en/of leeftijd

i) Bijzondere categorieën Persoonsgegevens (ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid)

j) Overige gegevens, namelijk (vul aan)

- Welke gevolgen kan de Inbreuk hebben voor de persoonlijke levenssfeer van de Betrokkenen?
(U kunt meerdere mogelijkheden aankruisen)

  a) Stigmatisering of uitsluiting

  b) Schade aan de gezondheid

  c) Blootstelling aan (identiteits)fraude

  d) Blootstelling aan spam of phishing

  e) Anders, namelijk (vul aan)

<u>Vervolgacties naar aanleiding van het Inbreuk in verband met Persoonsgegevens</u>

- Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

<u>Technische beschermingsmaatregelen</u>

- Zijn de Persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
(Kies een van de volgende opties en vul waar nodig aan)

  a) Ja

  b) Nee

  c) Deels, namelijk: (vul aan)

- Als de Persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?
  (Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Internationale aspecten

- Heeft de Inbreuk betrekking op personen in andere EU-landen?
  (Kies een van de volgende opties)

  a) Ja

  b) Nee

  c) Nog niet bekend