

Verwerkersovereenkomst

Naam	Kennisnet diensten (categorie C)
Versie	1.1
Datum	28 augustus 2018
Referentie	C/KDC-18-xxx

Deze verwerkersovereenkomst is conform de modelverwerkersovereenkomst zoals deze is bijgesloten als bijlage bij het convenant "Digitale onderwijsmiddelen en privacy 3.0".

Ondergetekenden:

Stichting Kennisset, gevestigd en kantoorhoudende aan de Paletsingel 32, 2718 NT Zoetermeer, hierbij vertegenwoordigd door de mevrouw M. Mulder-Wigmans, Directeur Operations, hierna te noemen: "Kennisset, Verwerker",

en

Het bevoegd gezag van xxx, geregistreerd onder bestuursnummer xxx bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan adres, te postcode woonplaats, te dezen rechtsgeldig vertegenwoordigd door functie, naam bevoegd gezag, hierna te noemen: "Onderwijsinstelling".

hierna gezamenlijk te noemen: "Partijen", of afzonderlijk: "Partij"

Overwegen het volgende:

- a) Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij Onderwijsinstelling Verwerker opdracht geeft om de door Verwerker zoals in de Privacy Bijsluiter omschreven Dienst te verlenen, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
- b) Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.
- c) Voor zover Partijen deze Verwerkersovereenkomst sluiten voor 25 mei 2018, gelden de relevante bepalingen uit de WBP.

verklaren te zijn overeengekomen als volgt:**Artikel 1. Definities**

In deze Verwerkersovereenkomst wordt verstaan onder:

- a) Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
- b) Bijlage(n): bijlage(n) bij het Convenant of de Verwerkersovereenkomst;
- c) Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy 3.0;
- d) Convenantpartij: een tot het Convenant toetgetreden Onderwijsinstelling of Leverancier;
- e) Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
- f) Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g) Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
- h) Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst. Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);

- i) Keten iD: een pseudoniem van een persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het Keten iD wordt ook ECK iD genoemd;
- j) Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;
- k) Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
- l) Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
- m) Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
- n) Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
- o) Product- en Dienstenovereenkomst: : de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a (voor Kennisnet gaat het hierbij om de 'Gebruiksvoorwaarden Kennisnet diensten'); Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
- p) Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
- q) School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem, studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerling volgsysteem;
- r) Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);
- s) Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
- t) AVG: de Algemene Verordening Gegevensbescherming (Verordening 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);
- u) Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) 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.

Artikel 2. Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in Bijlage 1, die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Onderwijsinstelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3. Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.
3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Onderwijsinstelling in Bijlage 1 over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in Bijlage 1 opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en) en de uitvoering van de bijbehorende Verwerkingen.
4. De Onderwijsinstelling neemt de in lid 2 van dit artikel genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.
5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.
6. Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4. Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5. Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechterlijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt

- Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking van dat wettelijke voorschrift dan wel de rechterlijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.
2. Een overzicht van onder meer de categorieën Persoonsgegevens en het doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacybijsluiter bij deze Verwerkersovereenkomst.
 3. De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de Verwerkersverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt
 4. Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.

Artikel 6. Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij betreft bij de Verwerking van Persoonsgegevens, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerkers, deze gegevens als vertrouwelijk behandelt. Verwerker waarborgt dat met de tot het Verwerken van de Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding zijn gebonden.
2. De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:
 - a) voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;
 - b) indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of
 - c) indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, tot verstrekking verplicht is.
3. Verwerker onthoudt zich van verstrekking of bekendmaking van Persoonsgegeven aan een Derde, tenzij deze verstrekking of bekendmaking plaatsvindt in opdracht van Onderwijsinstelling respectievelijk wanneer dit noodzakelijk is om te voldoen aan een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker - tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.
4. Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 7. Beveiliging en controle

1. Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
2. Naast de maatregelen als genoemd in artikel 32 lid 1 AVG, worden onder meer de volgende maatregelen - waar passend - genomen:
 - a. een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;
 - b. maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
 - c. het regelen van procedures rondom het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering, en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren.
3. Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
4. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze van de verklaringen die Verwerker verstrekt over de afgesproken beveiligingsmaatregelen.
5. De Verwerker stelt in goed overleg de Onderwijsinstelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken.
6. In aanvulling op de voorgaande leden heeft Onderwijsinstelling te allen tijde het recht om, in overleg met de Verwerker en met inachtneming van een redelijke termijn, de naleving van Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, de Product- en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde externe deskundige:
 - a. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.
 - b. De auditor verstrekt het auditrapport alleen aan Partijen.
 - c. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
 - d. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
 - e. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8. Datalekken

1. Partijen hebben een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover *zonder onredelijke vertraging* informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt in geval van een Datalek alle relevante informatie aan Onderwijsinstelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.
3. Verwerker informeert Onderwijsinstelling *onverwijld* indien een vermoeden bestaat dat een Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34, lid 1, AVG.
4. Verwerker stelt bij een Datalek de Onderwijsinstelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Onderwijsinstelling daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens, en meer in het bijzonder (verdere) schending van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, te voorkomen of te beperken.
5. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. In geval een Datalek bij Verwerker meerdere Onderwijsinstellingen in gelijke mate treft, kan Verwerker, na overleg met een of meerdere Verwerkingsverantwoordelijken, namens de Onderwijsinstellingen een melding doen van het Datalek aan de Autoriteit Persoonsgegevens. Van het voornemen hiervan zal Verwerker Onderwijsinstelling onverwijld (en zo mogelijk voorafgaand aan de melding) in kennis stellen.
6. In geval van het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Onderwijsinstelling de Betrokkenen informeren over het Datalek.
7. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.
8. Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.
9. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e van deze Verwerkersovereenkomst, informeert de Verwerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9. Bijstand

1. Verwerker verleent Onderwijsinstelling bijstand bij het doen nakomen van de op Onderwijsinstelling rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking - maar niet beperkt - tot:
 - a. het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
 - b. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
 - c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortvloeiende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
 - d. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
 - e. het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.

2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

Artikel 10. Doorgifte aan derde landen buiten de Europese Economische Ruimte

1. Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land of internationale organisatie indien Onderwijsinstelling daarvoor specifieke Schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Onderwijsinstelling voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
2. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de Europese Economische Ruimte of aan een internationale organisatie zoals bedoeld in artikel 4 lid 26 AVG, dan zien Partijen er op toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien gegevens worden doorgegeven aan een derde land of een internationale organisatie, dan wordt dit in Bijlage 1 bij deze Verwerkers-overeenkomst aangegeven, inclusief een opgave van de landen waar, of internationale organisaties door wie, de Persoonsgegevens worden verwerkt. Daarbij wordt tevens aangegeven op welke wijze is voldaan aan de voorwaarden op basis van de AVG voor doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

Artikel 11. Inschakeling Subverwerker

1. Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkers-overeenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in de Privacybijsluiters.
2. Tijdens de duur van de Verwerkersovereenkomst licht Verwerker Onderwijsinstelling in over een voorgenomen toevoeging van een nieuwe Subverwerker of wijziging in de samenstelling van de bestaande Subverwerkers, waarbij Onderwijsinstelling de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
3. Verwerker is verplicht iedere Subverwerker via een overeenkomst of andere rechtshandeling minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd. Hieronder vallen onder meer de verplichting om de Persoonsgegevens niet verder te Verwerken anders dan in het kader van deze Verwerkersovereenkomst is overeengekomen, en de verplichting tot het nakomen van de geheimhoudingsverplichtingen, meldingsverplichtingen, medewerkingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens zoals in deze Verwerkersovereenkomst vastgelegd. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Verwerkers-overeenkomsten, of van de relevante passages uit de Verwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 11, lid 1, van deze overeenkomst ingeschakelde Subverwerker.

Artikel 12. Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
3. Verwerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Verwerker zal alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkers-overeenkomst en zal waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13. Aansprakelijkheid

1. Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Product- of Dienstenovereenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:
 - a. verhaalsactie op grond van artikel 82 AVG; of
 - b. schadevergoedingsactie uit hoofde van deze Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthouder betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken partij op grond van de geldende wet- of regelgeving ter beschikking staat.

2. Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 14 lid 2.
3. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthouder, beiden in verband met deze Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 14. Tegenstrijdigheid en wijziging Verwerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Verwerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Verwerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens en de

doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in Bijlage 1 worden opgenomen.

4. Wijzigingen in de artikelen van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 15. Duur en beëindiging

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 5, lid 1, en de artikelen 6, 9 en 12.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Stichting Kennisnet,

Onderwijsinstelling,

Naam: M. Mulder-Wigmans
Functie: Directeur Operations

Naam:
Functie:

Datum: 28 augustus 2018

Datum: 28 augustus 2018

*Bijlage Dienst
Bijlage 1: SLS*

BIJLAGE 1: PRIVACYBIJSLUITER Nummervoorziening

Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals onderwijsdeelnemers). Onderwijsinstellingen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiters geeft onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag “wie, wat, waar, waarom en hoe” wordt omgegaan met de privacy van de betrokken personen van wie persoonsgegevens worden verwerkt.

Het gebruik van deze Privacybijsluiters helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. De Privacybijsluiters is een bijlage bij de Modelverwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.

A. Algemene informatie

Naam product en/of dienst	:	Nummervoorziening
Naam Verwerker en vestigingsgegevens	:	Stichting Kennisset, Zoetermeer
Link naar leverancier en/of productpagina	:	www.kennisset.nl/nummervoorziening/
Beknopte uitleg en werking product en dienst	:	De dienst genereert unieke, persistente, niet direct tot de persoon herleidbare Ketenpseudoniemen ten behoeve van het onderwijs in Nederland.
Doelgroep (zoals po/vo, onderbouw/bovenbouw)	:	Onderwijsinstellingen in het po, vo en mbo
Gebruikers	:	Onderwijsinstelling en de door hen ingeschakelde leveranciers

B. Omschrijving specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:

1. Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.
 - a. Het verwerken van aangeleverde gehashte identificerende gegevens van leerlingen en/of medewerkers van onderwijsinstellingen.
 - b. Het genereren van Stam- en Ketenpseudoniemen op grond van de aangeleverde gehashte identificerende gegevens.
 - c. Het vastleggen van alle binnenkomende aanvragen en de verwerking daarvan in logbestanden, voor gebruik door auditors en beheerders van de dienst. Van de binnenkomende aanvragen en verwerkingen wordt vastgelegd:
 - 1) De datum en het tijdstip van de aanvraag of verwerking
 - 2) Het BRIN en bestuursnummer van de aanvragende onderwijsinstelling
 - 3) Een kenmerk van de keten en de onderwijssector waarvoor de aanvraag wordt gedaan
 - 4) De laatste 6 karakters van de gehashte identificerende gegevens
 - 5) Een identificerend kenmerk van de leverancier van het koppelande systeem
 - 6) Een uniek kenmerk voor elke verwerking en voor de stap binnen de verwerking
 - 7) Deze logbestanden kunnen niet worden gewijzigd en worden maximaal 6 maanden bewaard, tenzij auditors redenen hebben om de logbestanden langer te bewaren.
2. Omschrijving van de optionele Verwerkingen die de Verwerker aanbiedt:
 - a. Het tijdelijk opslaan van de resultaten van bulkaanvragen (verzamelingen gehashte identificerende gegevens van leerlingen) voor Stam- en Ketenpseudoniemen. Deze resultaten worden opgeslagen gedurende maximaal 24 uur of totdat het aanvragende systeem de resultaten opvraagt. De resultaten bevatten de volgende gegevens:
 - 1) Het BRIN en bestuursnummer van de aanvragende onderwijsinstelling
 - 2) Een kenmerk van de keten en de onderwijssector waarvoor de aanvraag wordt gedaan

- 3) Een index uit de aanvraag, gekoppeld aan ofwel het volledige ECK ID dat gegenereerd is of een foutmelding waarom het ECK ID voor de invoer niet kon worden gemaakt.
- b. Het opslaan van gehashte identificerende gegevens van leerlingen die vanwege een wijziging in hun inschrijving in de Basisregister Personen beschikken over nieuwe identificerende gegevens (bijvoorbeeld, de overgang van een onderwijsnummer naar PGN of ten gevolge van de wijziging van een PGN).
 - 1) Het gehashte oude PGN en gehashte nieuwe PGN
Deze gegevens worden bewaard gedurende tenminste het verblijf van de leerling in de onderwijssector. Door de koppeling tussen het nieuwe gehashte identificerende gegeven en het uitgegeven Ketenpseudoniem worden conflicten tussen beide identiteiten voorkomen, zo behoudt de leerling een persistent Ketenpseudoniem.

C. Doeleinden voor het verwerken van gegevens

De Verwerker dient in deze Bijsluiter expliciet aan te geven of deze:

- I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of
- II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

Ad I. Indien de Verwerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

- a. het met gebruikmaking van het Digitale Onderwijsmiddel geven en volgen van onderwijs en het begeleiden en volgen van Onderwijsdeelnemers, waaronder:
 - * de opslag van leer- en toetsresultaten;
 - * het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;
 - * de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;
 - * analyse en interpretatie van leerresultaten;
 - * het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.
- b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
- c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
- d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.
- e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
- f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
- g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
- h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
- i. De uitvoering of toepassing van een andere wet

Ad II. (Alleen) indien de Verwerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

a. de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:

- ~~• de indeling en aanpassing van roosters;~~
- ~~• de analyse en interpretatie van leerresultaten;~~
- ~~• het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;~~
- ~~• het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;~~
- ~~• de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;~~
- ~~• financieel beheer;~~
- ~~• monitoring en verantwoording, ten behoeve van met name: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;~~
- ~~• het behandelen van geschillen.~~
- ~~• het uitwisselen van Persoonsgegevens met Derden, waaronder:

 - ~~• toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;~~
 - ~~• samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;~~
 - ~~• partijen betrokken bij de invulling van stage of leer- / werkplekken voor zover noodzakelijk en wettelijk toegestaan;~~
 - ~~• Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgenderwijs.~~~~

~~b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;~~

~~c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;~~

d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens.

e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;

~~f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;~~

~~g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.~~

h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.

i. De uitvoering of toepassing van een andere wet

D. Categorieën en soorten persoonsgegevens

1. Omschrijving van de categorieën Betrokkenen over wie Persoonsgegevens worden verwerkt, en de categorieën persoonsgegevens van de Betrokkenen:

Van toepassing	Categorie	Toelichting
n.v.t.	1. Contactgegevens	naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens; Beperkte set = naam, e-mail, opleiding; Persoonlijke set = geboortedatum, geslacht;
n.v.t.	2. Onderwijs- of deelnemersnummer	een administratienummer dat onderwijsdeelnemers identificeert
n.v.t.	3. Nationaliteit en geboorteplaats	
n.v.t.	4. Ouders, voogd	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
n.v.t.	5. Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
n.v.t.	6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
n.v.t.	7. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: <ul style="list-style-type: none"> • klas / leerjaar / ILT code • Examinering • Studievoortgang en/of Studietraject • Begeleiding onderwijsdeelnemers, inclusief handelingplan • Aanwezigheidsregistratie
n.v.t.	8. Onderwijsorganisatie	gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
n.v.t.	9. Financiën	gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en leskosten en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, alsmede bankrekeningnummer van de betrokkene;
n.v.t.	10. Beeldmateriaal	foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;
n.v.t.	11. Docent, zorgcoördinator, intern begeleider, decaan, mentor	gegevens van docenten en begeleiders , voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;
ja	12. Overige gegevens, te weten	Gehashte (niet direct tot de persoon herleidbare) identificerende gegevens van leerlingen zoals, maar niet beperkt tot, het hPGN. Gehashte (niet direct tot de persoon herleidbare) identificerende gegevens van medewerkers van onderwijsinstellingen zoals maar niet beperkt tot: een Globally Unique Identifier (GUID).
n.v.t.	13. BSN/PGN	
ja	14. Keten-ID (ECK-ID)	Dienst genereert een unieke iD voor de 'educatieve contentketen'. hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

2. Door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen):

Zie hiervoor onder B. voor een omschrijving van de gelogde gegevens

E. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

Amsterdam, Nederland

F. Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.

Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

Hostingprovider Vancis C&MS (vancis.nl), gevestigd te Amsterdam. Plaats/land van opslag en Verwerking Persoonsgegevens zie onder E.

Opmerking: indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiters of de werking van dit product of deze dienst, kunt u terecht bij:

Bezoekadres Nummervoorziening (Kennisset)

Stichting Kennisset
Paletsingel 32
2718 NT Zoetermeer

Postadres

Stichting Kennisset
Postbus 778
2700 AT Zoetermeer

Servicedesk

ondersteuning bij gebruik van en aansluiting op Nummervoorziening, tips en verbeteringsuggesties.

Telefoon: 0800-321 22 33 (op werkdagen van 9.00 – 17.00 uur)

E-mail : support@kennisnet.nl

G. Versie

Versie 1.0 15 maart 2018

Deze Privacybijsluiters maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <http://www.privacyconvenant.nl>.

BIJLAGE 2: BEVEILIGINGSBIJLAGE

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Normen informatiebeveiliging

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en op welke wijze passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.

Verwerker kan ook gebruik maken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging, mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

Minimale beveiligingsmaatregelen en aantoonbaarheid

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

1. (groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:

- a. De Nummervoorziening wordt gehost in een datacenter onder beheer van Vancis. Het datacenter in Amsterdam heeft een 24x7 op locatie aanwezige bewaking. Het datacenter is gevestigd op het Science Park Amsterdam, een terrein dat in eigendom is van NWO (Nederlandse Organisatie voor Wetenschappelijk onderzoek) en verboden terrein voor onbevoegden. In de avond vanaf 19.00 wordt het terrein hermetisch afgesloten door een omheind hek dat gesloten wordt. Bovendien heeft Vancis 24 x 7 een beveiligingsbedrijf dat toezicht houdt op het gehele terrein vanuit het Vancis datacenter. Zowel het terrein in Amsterdam als beide datacentra van Vancis zijn voorzien van camera's die voortdurend onder toezicht staan van de bewaking in het datacentrum Amsterdam. Het terrein en het datacenter zijn 24x7 toegankelijk voor personeelsleden van Vancis en voor bevoegd en aangemeld personeel van klanten of door klanten ingehuurde derden (aanmelding en legitimatie vereist). Kennisset is eigenaar van de hardware, en beheerders van Vancis hebben geen toegang tot de applicaties die draaien op de servers.
- b. De Nummervoorziening wordt beheerd volgens de bedrijfseisen voor toegangsbeveiliging van Kennisset. Gebruikers mogen via de netwerken van Kennisset alleen toegang krijgen tot die ICT-diensten, waarvoor zij specifiek geautoriseerd zijn. In de Kennisset netwerken dienen maatregelen te worden getroffen om groepen ICT-diensten, gebruikers en informatiesystemen te scheiden, ter bescherming van ongeautoriseerde toegang door andere netwerkgebruikers.
- c. Maatregelen
 - Binnen de OCC is er VLAN scheiding aangebracht tussen diensten en tussen frontend en backend netwerken.
 - Toegang vanaf OCC naar internet en vanaf internet naar OCC is standaard altijd geblokkeerd, tenzij expliciet gewhitelist
 - Toegang vanaf de vaste netwerk verbindingen op het Kennisset kantoor naar OCC (over 'gewoon' internet) is standaard toegestaan op oa. http, https, ssh en rdp
 - Binnen het kantoor is er VLAN scheiding tussen het servernetwerk, bedrade kantoor apparatuur en tussen de verschillende wifi netwerken
 - Van alle kantoor diensten zijn webdiensten gemaakt die vanaf internet direct te benaderen zijn
 - Accounts kunnen alleen aangevraagd worden door een geautoriseerde persoon binnen de organisatie met toegang tot het betreffende systeem

- Accounts worden alleen aangemaakt mits de functie van de persoon waarvoor het account wordt aangevraagd deze toegang vereist en de functie deze toegang rechtvaardigt.
- d. De applicatie heeft een aantal maatregelen tbv autorisatie geïmplementeerd. De architectuur van de Nummervoorziening kent vier onderdelen:
 - Een web service
 - Een beheerapplicatie
 - Een batch applicatie voor bulk verwerking
 - Een gemeenschappelijke database
- **De web service** biedt toegang tot de onder specifieke diensten B lid 1 en 2 genoemde functionaliteiten. Deze service is toegankelijk voor SOAP requests afkomstig van gekwalificeerde aanbieders van LAS systemen zoals beschreven in E van de privacybijsluiters en van scholen waarvan het bestuur deze overeenkomst heeft onderschreven. De identiteit van de aanbieder wordt bij elk verzoek vastgesteld aan de hand van een cryptografisch certificaat dat de aanbieder meestuurt als onderdeel van het verzoek. De identiteit van de school wordt vastgesteld aan de hand van een veld uit het bericht. Alle binnenkomende verzoeken worden gelogd.
- **De beheerapplicatie** geeft toegang tot de autorisatie- en inzagefunctionaliteiten van de Nummervoorziening:
 1. Inzien en aanpassen van bulkaanvragen volgens specifieke diensten onder B. 2. a: status inzien en handmatig verwijderen van bulkaanvragen en resultaten van de bulkverwerking. Het is niet mogelijk om de individuele ghashte PGNs in een bulk aanvraag te zien of te wijzigen.
 2. Inzien en handmatig verwijderen van substituties volgens specifieke diensten B. 2. b: zien van de laatste 6 tekens van het oude en nieuwe PGN, identificatie van de aanvragende school en LAS-systeem, datum en tijdstip van de aanvraag
 3. Inzien, autoriseren en autorisaties intrekken voor aanbieders van LAS systemen
 4. Inzien, autoriseren en autorisaties intrekken van schoolbesturen
 5. Inzien van gegevens van scholen
 6. Verversen van gegevens van scholen en schoolbesturen vanuit de open data van DUO
 7. Inzien van de log-gegevens van de web service en van de beheerapplicatie. De logbestanden bevatten de informatie beschreven in specifieke diensten B. 1. c.
- **De batch applicatie** verwerkt binnengekomen bulk aanvragen voor het genereren van stam-pseudoniemen en ECK IDs. De batch applicatie bevat geen functionaliteit voor gebruikers. De batch applicatie wordt periodiek en geautomatiseerd aangeroepen.
- **De gemeenschappelijke database** bevat de administratie van alle deelsystemen alsmede de gegevens van de substituties beschreven in specifieke diensten B. 2. b.
- De Beheerapplicatie van de Nummervoorziening wordt restrictief aangeboden aan medewerkers met beheer-rollen. Om dit te ondersteunen zijn diverse maatregelen van kracht, zowel op infrastructureel als logisch niveau.
- Beveiliging op infrastructureel niveau: Op basis van IP-whitelisting wordt toegang tot de Beheerapplicatie op netwerkniveau ingeperkt tot alleen toegankelijk vanuit het kantoor van Kennisset. Daarnaast wordt voor de Beheerapplicatie voorzien in authenticatie op basis van Entree Federatie, waarbij de gebruiker een geldige Digicode voor de rol Admin en/of Auditor moet bezitten. Communicatie zal plaatsvinden over een beveiligde verbinding.
- Alleen geautoriseerde gebruikers kunnen gebruik maken van de Beheerapplicatie. Een beheerder met de juiste rechten in het systeem kan een nieuwe beheerder aanmaken door het registreren van

zijn Kennisnet Entree Federatie UID. De nieuwe beheerder ontvangt een e-mail met een tijdelijk wachtwoord, welke hij binnen een bepaalde tijd dient te wijzigen.

- De Beheerapplicatie werkt middels rollen. Elke beheerder is gekoppeld aan één specifieke rol. Een rol omvat autorisaties, waarmee kan worden aangegeven welke functionaliteit beschikbaar is voor de rol.

2. Handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

De beheerapplicatie kent twee rollen: beheer en auditor. Beheerders hebben toegang tot alle functionaliteit genoemd onder 'De beheerapplicatie' hierboven. Auditors hebben toegang tot functionaliteit 7 genoemd onder 'De beheerapplicatie' hierboven.

Technisch beheerders van Kennisnet hebben toegang tot de gemeenschappelijke database van de Nummervoorziening en tot de operating systemen van de systemen waar de Nummervoorziening op draait. Technisch beheerders van Kennisnet vallen onder de voorschriften genoemd in I.1 leden a t/m c.

II. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Kennisnet hanteert de norm ISO 27001:2013 en bijbehorende werkwijzen als norm voor informatiebeveiliging. Het applicatieplatform waarop de Nummervoorziening wordt gehost is het Kennisnet standaard Linux platform, dat gehardend is.

De serviceapplicatie maakt gebruik van beveiligingsmaatregelen voor software zoals input-verificatie en validatie van tokens voor autorisatie van beheerders.

III. Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

Kennisnet heeft in 2016 het ISO 27001:2013 certificaat verkregen. Onderdeel van deze certificering is een reguliere jaarlijkse externe audit op richtlijnen en verbeterpunten.

Rapportage (artikel 7.4 van de Verwerkersovereenkomst)

Kennisnet rapporteert periodiek over de door Kennisnet genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.

Informeren en melding Datalekken en/of incidenten met betrekking tot beveiliging

- Kennisnet hanteert intern een vastgestelde procedure voor het vaststellen en afhandelen van beveiligingsincidenten.
 - Een incident wordt vastgesteld door gebruikers van de dienst, technisch beheerders van de dienst of door eigenaars van de dienst. Technisch beheerders maken hierbij gebruik van logging ingebouwd in de Nummervoorziening. De servicedesk blijft aanspreekpunt voor verdere informatie.
 - Elk incident wordt gemeld aan de servicedesk, dit kan per telefoon en per email. De servicedesk maakt een ticket aan en zet de melding door naar de security officer van Kennisnet (SO).
 - Afhankelijk van de prioriteit en impact zal de SO:
 - Het incident melden bij de functionaris voor gegevensbescherming (die de verdere communicatie met Autoriteit Persoonsgegevens en zo nodig verantwoordelijken op zich neemt)
 - Binnen Kennisnet informeren van CTO, eigenaar en andere betrokkenen van de dienst.
 - De SO formeert een task force die het incident analyseert en eventueel oplost. Als de melding is verhopend, stelt deze hierover een rapport op met alle bijzonderheden van het incident.

- In geval van een Datalek waarbij de oorzaak daarvan ligt bij de dienst, waarbij er meerdere verantwoordelijken (onderwijsinstellingen) door het Datalek getroffen zijn, zal Kennisnet met die verantwoordelijken overleg voeren. Kennisnet zal voor de verantwoordelijken zorg dragen voor melding van het Datalek bij de Autoriteit Persoonsgegevens. Kennisnet zal de verantwoordelijken hierover zo spoedig mogelijk informeren.

Informatie die in ieder geval over een incident gedeeld moet worden

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van het beveiligingsincident;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met:

Kennisnet servicedesk

Telefoon : 0800-321 22 33 (op werkdagen van 9.00 – 17.00 uur)

E-mail : servicedesk@kennisnet.nl

De contactpersoon voor Verwerker is: Robert Klein

Versie

Versie 1.0 15 maart 2018

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <http://www.privacyconvenant.nl>.