

Model Verwerkersovereenkomst 3.0

Deze Model Verwerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

De nieuwe Model Verwerkersovereenkomst 3.0 komt in de plaats van eerdere Model verwerkersovereenkomsten uit 2015 en 2016. De uitgangspunten van deze Model Verwerkersovereenkomst 3.0 sluiten aan bij de bepalingen in het Convenant, geven invulling aan verplichtingen op grond van de Europese Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals onder andere in (inter)nationale beveiligingsnormen, jurisprudentie en richtsnoeren van de toezichthouder zijn aangegeven.

Reeds afgesloten Verwerkersovereenkomsten op basis van de modellen uit 2015 en 2016 blijven hun gelding houden totdat deze verwerkersovereenkomsten door partijen worden beëindigd. Het uitgangspunt is dat met ingang van 25 mei 2018, het moment waarop de AVG van toepassing wordt, Onderwijsinstellingen en Leveranciers bij het aangaan van een verwerkersovereenkomst of bij vernieuwing van een bestaande verwerkersovereenkomst, de Model Verwerkersovereenkomst 3.0. gebruiken.

In het Convenant is afgesproken dat Onderwijsinstellingen en Leveranciers het actuele model gebruiken bij het maken van afspraken. Van de actuele Model Verwerkersovereenkomst kan alleen gemotiveerd en schriftelijk worden afgeweken.

Deze Model Verwerkersovereenkomst 3.0 bevat twee bijlagen:

1. In de Privacybijsluiters (Bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
2. In de Beveiligingsbijlage (Bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model Verwerkersovereenkomst is te vinden op de website www.privacyconvenant.nl. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad, VO-raad, MBO Raad (saMBO-ICT) en bij Kennisnet.

Maart 2018

Partijen:

1. Het bevoegd gezag van <naam + rechtsvorm onderwijsinstelling>, geregistreerd onder BRIN-nummer <brin> bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: **"Onderwijsinstelling"**.

en

2. De bewerker

Naam: Peuter-kleuterpraktijk Ellen Voogt
Straat: Verfmolen 22
Postcode: 3146CX
Plaats: Maassluis

Rechtsgeldig vertegenwoordigd door: E.P.Voogt-van den Berg, onderwijsadviseur en eigenaar van "BOSOS"

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

Overwegen het volgende:

- a. De Onderwijsinstelling en de Peuter-kleuterpraktijk Ellen Voogt zijn een overeenkomst aangegaan voor het gebruik van het door de Peuter-kleuterpraktijk Ellen Voogt aangeboden leerling volgsysteem "BOSOS". De peuter-kleuterpraktijk biedt de Onderwijsinstelling de mogelijkheid om de leerlingen te volgen in hun ontwikkeling en handelingsplannen en/of rapportage te maken. Dit is vastgelegd in de Product- en Dienstenovereenkomst, hierna te noemen Overeenkomst "BOSOS", die wordt afgesloten tussen de Onderwijsinstelling en de Peuter-kleuterpraktijk Ellen Voogt. Dat contract leidt ertoe dat de Onderwijsinstelling gegevens van leerlingen en gebruikers aanlevert die door de Onderwijspraktijk worden ingevoerd en bewerkt in "BOSOS".
- 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.

Komen het volgende overeen:

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 toegetreden 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 Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;
- p. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
- q. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
- r. 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;
- s. 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);

- t. 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;
- u. 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);
- v. 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 voorafgaande 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 verwerkingsactiviteiten¹ 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: Privacyconvenant

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 Privacybijsluiters bij deze Verwerkersovereenkomst.
3. De Verwerker dient in de Privacybijsluiters aan te geven of de Privacybijsluiters ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiters 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.
5. *SPECIEFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT: In aanvulling op het bepaalde in lid 4, is het Verwerker uitsluitend toegestaan om Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde andere onderwijsinstelling, na een concreet verzoek tot verstrekking van die onderwijsinstelling*

¹ Zie voor een voorbeeld de Aanpak IBP bij <https://kn.nu/IBPonderwijs>

en op voorwaarde dat deze andere onderwijsinstelling haar administratieve onderwijsidentiteit (bijv. BRIN of OiN) aan Verwerker kenbaar heeft gemaakt. Indien de andere onderwijsinstelling niet beschikt over een administratieve onderwijsidentiteit zal Verwerker Persoonsgegevens alleen aan die andere onderwijsinstelling verstrekken op uitdrukkelijke instructie van Onderwijsinstelling.

6. SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS:
- a. *Convenantspartijen die Leermiddelen en Toetsen ontwikkelen en aanbieden (hierna te noemen: **Leermiddelenleverancier**), zullen jaarlijks ten behoeve van het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, (welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld) de Privacy Bijsluiter voor die Leermiddelen en Toetsen aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt (met betrekking tot de Leermiddelen en Toetsen die op de desbetreffende leermiddelenlijsten worden opgenomen).*
 - b. *Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.*
 - c. *De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.*
 - d. *Onderwijsinstelling vrijwaart Verwerker (distributeur) voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Leermiddelenleverancier, en de Onderwijsinstelling vrijwaart de Leermiddelenleverancier voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Verwerker (distributeur).*
 - e. *De verantwoordelijkheid van Verwerker (distributeur) voor het beheer van de Persoonsgegevens houdt op, op het moment dat de Leermiddelenleverancier die gegevens heeft ontvangen van Verwerker (distributeur).*

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 ingeval 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 voortkomende 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 Privacybijsluiter.
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 Verwerkersovereenkomst 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,

Onderwijsinstelling,

Verwerker,

Naam:

Naam: E.P.Voogt-van den Berg

Functie:
Voogt

Functie: Directeur Peuter-kleuterpraktijk Ellen

Datum:

Datum: 1 april 2018

Bijlage 1: Privacybijsluiters

Bijlage 2: Beveiligingsbijlage

BIJLAGE 1: PRIVACYBIJSLUITER [BOSOS 2tot 4 en BOSOS]

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.

In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacybijsluiters. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: “Bijlage 1A”, “Bijlage 1B”, etc.. Deze Bijlagen worden aan de Verwerkersovereenkomst gehecht.

Voor specifieke branches zoals uitgevers, distributeurs en leveranciers van student- en leerling-administratiesystemen, kunnen specifieke privacybijsluiters worden gemaakt die gebaseerd zijn op dit model. Deze specifieke modellen zijn afgestemd door de Initiatiefnemers van het Convenant. De modellen zijn te vinden op de website van het Platform: www.edu-k.nl/ibp.

A. Algemene informatie

Naam product en/of dienst	: Leerling Volgstelsel “BOSOS” Webbased
Naam Verwerker en vestigingsgegevens	: Peuter-kleuterpraktijk Ellen Voogt Verfmolen 22 3146 CX Maassluis
Link naar <u>leverancier</u> en/of productpagina	: www.bosos.nl www.bosos2tot4.nl
Beknopte uitleg en werking product en dienst	: Met “BOSOS” volgen leerkrachten de ontwikkeling van hun leerlingen op sociaal-emotioneel, motorisch en cognitief gebied. Zij screenen de kinderen iedere drie maanden en kunnen indien nodig handelingsplannen maken. Op basis daarvan kan de intern begeleider begeleiding en ondersteuning bieden. Verder biedt het programma de mogelijkheid rapportages te maken die kunnen dienen om te evalueren en te verantwoorden.
Doelgroep (zoals po/vo, onderbouw/bovenbouw)	: Basisonderwijs en Speciaal Onderwijs
Gebruikers	Leerkrachten, intern begeleiders en directies scholen. Indien van toepassing administratieve krachten of ict-ers als beheerder.

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.

De overeenkomst: de specifieke schoolgegevens van de deelnemer aan "BOSOS" worden ingevoerd: naam school, BRIN nummer, naam directeur, adres, telefoon en emailadres en de contactpersoon voor "BOSOS". De school kan kiezen voor het hele programma of voor het werken zonder leerlingen vragenlijsten of met alleen leerlingen vragenlijsten.

2. Omschrijving van de optionele Verwerkingen die de Verwerker aanbiedt

De gebruikers worden via een lijst aangeleverd en door Bewerker ingevoerd. Zij worden ingevoerd met hun voornaam, achternaam, initialen, e-mailadres en gebruikersnaam. Hun rol wordt aangevinkt. Alleen die personen kunnen met hun e-mailadres een wachtwoord opvragen. De gebruikers zijn directie, leerkrachten, intern begeleiders en beheerders. Indien gewenst kunnen vakleerkrachten of adviseurs worden toegevoegd. Dit wordt bepaald door de Onderwijsinstelling zelf wie zij toegang verlenen. Iedere gebruiker krijgt een rol binnen "BOSOS" met bijbehorende rechten. Een leerkracht kan alleen het dossier bewerken. De andere gebruikers niet. Die hebben inzage recht.

Inhoud: via observaties wordt de ontwikkeling van de leerlingen gevolgd en wordt gekeken of er reden tot zorg is. Zo ja, dan kan de leerkracht een handlingsplan maken. Die gegevens worden per kind opgeslagen, maar kunnen ook worden gerelateerd aan de groep en aan de school. Op basis van die gegevens kunnen rapportages worden gemaakt voor intern gebruik in de school en voor verantwoording naar de Onderwijsinspectie.

Scholen die met Parnassys werken, kunnen gebruik maken van een koppeling waardoor leerlingen en groepen rechtstreeks uit Parnassys in "BOSOS" worden overgenomen. Scholen geven aan dat zij gebruik willen maken van de koppeling, Bewerker meldt de school aan in Parnassys en brengt de school op de hoogte hoe die koppeling geactiveerd kan worden. Daarmee geeft de school Parnassys toestemming de gegevens uit te wisselen.

Scholen die met andere leerlingen administratie systemen werken leveren via de site www.bososs.nl hun leerlingen aan m.b.v. EDEXML bestand.

Gebruikers worden via een nieuwsbrief op de hoogte gehouden van het aanbod van de Peuter-kleuterpraktijk Ellen Voogt. Dit aanbod is gericht op het primaire leerproces van de onderwijsinstelling. Iedere gebruiker heeft de mogelijkheid zich af te melden voor de nieuwsbrief.

Belangrijke mededelingen die met "BOSOS" te maken hebben, worden op de voorpagina (zichtbaar na het inloggen), geplaatst.

Aan Ellen Voogt kan in het kader van een opdracht tijdelijk toegang tot het systeem worden verleend op uitdrukkelijk verzoek en met toestemming van het bevoegd gezag van de scholen. Het enige doel daarvan is analysering van de door de gebruikers ingevoerde gegevens op basis waarvan advies gegeven kan worden aan directie en team van een school. Doel daarvan is kwaliteitsverbetering en deskundigheidsbevordering wat betreft de aanpak van gedrag- en werkhoudingsproblemen. Na afloop van de opdracht wordt de toegang weer beëindigd.

Voor problematische groepen kan een eenmalige overeenkomst worden afgesloten om de problemen in kaart te brengen en op basis daarvan plannen te maken. Hiervoor kan een van tevoren gekozen aantal leerlingen worden ingevoerd.

MBO

Toelichting: Het gaat hier om aanvullende diensten en bijhorende Verwerkingen die geen onlosmakelijk onderdeel vormen van de aangeboden dienst. Dit zijn bijvoorbeeld optionele diensten voor de Onderwijsinstelling die behulpzaam kunnen zijn voor de Onderwijsinstelling t.b.v. het primaire (leer)proces en administratieve werkzaamheden.

De Onderwijsinstelling dient een keuze te maken en daarbij opdracht te geven om persoonsgegevens te verwerken, voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box).

De opdracht kan ook worden verleend doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te doen.

C. Doeleinden voor het verwerken van gegevens

1. het toegang krijgen tot en in gebruik kunnen nemen van “BOSOS”
2. analyse en interpretatie van de observaties
3. bijhouden van persoonlijke gegevens (waaronder medische) van een leerling en de eventuele gevolgen daarvan voor de algemene ontwikkeling
4. het begeleiden en ondersteunen van leerkrachten binnen de Onderwijsinstelling
5. communicatie met leerlingen, ouders en medewerkers van de Onderwijsinstelling
6. monitoring en verantwoording ten behoeve van de Onderwijsinstelling zelf
7. het uitwisselen van die gegevens met derden (zoals diverse commissies) waarvoor de Onderwijsinstelling toestemming verleent
8. overzetten van een leerling naar een andere school die ook met “BOSOS” werkt op verzoek van de Onderwijsinstelling
9. tijdelijke gebruikers toevoegen zoals vakleerkrachten of remedial teachers
10. continuïteit en goede werking van “BOSOS” volgens de licentie overeenkomst. Hieronder valt het oplossen van problemen mits niet veroorzaakt door de Onderwijsinstelling, de helpdeskfunctie en het oplossen van geconstateerde fouten

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
	1. Contactgegevens	1. naam school, naam directeur, BRINnummer, adres, telefoongegevens, e-mailadres, contactpersoon

	2. Onderwijs-deelnemer-nummer	2. Registratie van leerlingen met hun naam, geboortedatum en geslacht.
	3. Nationaliteit en geboorteplaats	n.v.t
	4. Ouders, voogd	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;
	6. Godsdienst	n.v.t
	7. Studievoortgang	n.v.t
	8. Onderwijsorganisatie	n.v.t
	9. Financiën	n.v.t
	10. Beeldmateriaal	n.v.t.
	11. Docent, zorg-coördinator, 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;
	12 Overige gegevens, te weten	De gebruikers worden via een nieuwsbrief op de hoogte gehouden van het aanbod gericht op onderwerpen die voortvloeien uit "BOSOS". Die gegevens worden niet verstrekt aan andere leveranciers of aan derden.
	13. BSN/PGN	n.v.t
	14. Keten-ID (ECK-ID)	Brinnummer

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

De persoonsgegevens worden door de onderwijsinstelling beheerd]

E. Opslag Verwerking Persoonsgegevens:

Land van opslag en verwerking van de gegevens: server en backup server staan op verschillende plaatsen in Nederland zodat bij een calamiteit niet alle gegevens verloren gaan wanneer ze op één plaats ondergebracht zouden zijn.

F. Subverwerkers

1. Bewerker maakt voor “BOSOS” gebruik van de volgende Subbewerker:
Internetbureau Netgemak, Stationsplein 69, 7551 CR Hengelo.
Zij hebben “BOSOS” technisch ontwikkeld en doen de hosting van het programma. Zij verzorgen het onderhoud van het programma, voeren in opdracht van de Peuter-kleuterpraktijk Ellen Voogt aanpassingen en updates uit en verzorgen de helpdeskfunctie voor technische vragen. Om dat te kunnen doen heeft Netgemak de functie van Administrator en kunnen zij bij alle onderdelen van “BOSOS”. Tevens zijn zij contactpersoon voor de koppeling van “BOSOS” met Parnassys. Met Netgemak is een subbewerkerovereenkomst afgesloten

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiters of de werking van dit product of deze dienst, kunt u terecht bij: [Peuter-Kleuterpraktijk Ellen Voogt] info@peuter-kleuterpraktijk.nl

G. Versie

versie 3.0 1 mei 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.

Voor het toepassen en aantonen van de technische maatregelen, kan Verwerker gebruik maken van (zo snel als redelijkerwijs mogelijk de meest recente versie van) het in het onderwijs ontwikkelde '*Certificeringsschema informatiebeveiliging en privacy ROSA*'². Dat schema voorziet in een baseline van (beveiligings)maatregelen waarmee organisaties dit aantoonbaar kunnen maken.

Indien Verwerker voornoemd Certificeringsschema gebruikt, dan mag gebruik worden gemaakt van een standaard beveiligingsbijlage die is afgestemd door de Initiatiefnemers van het Convenant. Deze afgestemde bijlage 2 is te vinden op de website van het Platform en komt in de plaats van deze model bijlage 2: www.edu-k.nl/ibp.

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

In deze bijlage staan alle maatregelen die Bewerker heeft genomen voor de bewaking van de vertrouwelijkheid, integriteit en beschikbaarheid. Onderstaand verklaring van de termen.

- *Vertrouwelijkheid*: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
- *Integriteit*: het waarborgen van de correctheid en volledigheid van de informatie alsook de verwerking daarvan.
- *Beschikbaarheid*: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie.

1. Begrippenlijst.

In dit document worden de volgende begrippen gebruikt:

Beveiligingsincident (datalek)

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie in gevaar is of kan komen.

² <https://www.edustandaard.nl/standaard-afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/>

Back-up

Een back up is een reservekopie van de gegevens die zich binnen een applicatie bevinden.

HTTPS

HTTPS is de afkorting van Hyper Tekst Transfer Protocol Secure. Dit is een uitbreiding van het http protocol waarmee de verbinding met behulp van SSL encryptie wordt versleuteld. Http is een communicatie protocol waarmee een cliënt systeem met een server systeem communiceert om gegevens uit te wisselen.

SaaS

SaaS is een afkorting van Software as a Service. SaaS betekent dat de software die nodig is voor dataverwerking reeds is geïnstalleerd en gehost aangeboden wordt. De dienst is direct beschikbaar via het web.

SFTP

SFTP is de afkorting voor SSH File Transfer Protocol. Dit is een uitbreiding van het FTP protocol waarmee de verbinding via een SSH verbinding wordt getunneld. FTP is een communicatie protocol waarmee een cliënt systeem met een server systeem communiceert om bestanden uit te wisselen.

SSL

SSL is de afkorting van Secure Sockets Layer, het meest gebruikte beveiligingsprotocol.

2. Maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

De applicatie “BOSOS” is een SAAS oplossing. Het beheer en onderhoud worden uitsluitend door daartoe geautoriseerde personen uitgevoerd.

2.1 Toegang

Gebruikerstoegang is enkel mogelijk door in te loggen op de online applicatie. De verbinding maakt gebruik van TLS 1.2 en gecodeerd en geverifieerd met AES_128_GCM en gebruikt ECDHE_RSA als mechanisme voor sleuteluitwisseling. Het algoritme voor de handtekening is sha256RSA. De openbare sleutel is RSA (2048 Bits).

De volgende mensen hebben toegang tot de software en de daarin opgeslagen persoonsgegevens met de handelingen die zij uitvoeren:

- De eigenaren van de Peuter-kleuterpraktijk Ellen Voogt als beheerder van “BOSOS”. Zij hebben toegang tot alle administratieve gegevens maar niet tot de leerling gegevens. Die zijn toegankelijk nadat de school daar schriftelijk toestemming voor heeft gegeven. De Peuter-kleuterpraktijk Ellen Voogt vervult tevens de helpdeskfunctie, pr-activiteiten en facturering.
- Ellen Voogt in haar rol als onderwijsadviseur. Zij adviseert bij inhoudelijke vragen en analyseert gegevens in opdracht van de Onderwijsinstelling.
- Medewerkers Netgemak voor het ontwikkelen van software, updaten en testen en de admin-functie. Tevens zijn zij de technische helpdesk voor de Onderwijspraktijk. Ook zijn zij verantwoordelijk voor de koppeling met Parnassys.
- Beheerders namens de Onderwijsinstelling. Zij zijn gebruikers met eigen rechten maar kunnen die rechten ook delegeren naar andere gebruikers. Zij kunnen gebruikers, groepen en leerlingen aanmaken en verwijderen en gegevens aan elkaar koppelen.
- Gebruikers van de applicatie hebben toegang tot het dashboard. Hier worden alle gegevens waarvoor zij geautoriseerd zijn voor hen ontsloten. Gebruikers zijn altijd gekoppeld aan de Onderwijsinstelling en kunnen geen toegang krijgen tot het dashboard van andere Onderwijsinstellingen.
- De “BOSOS” beheerders hebben de machtigingen om te bepalen welke gegevens via het dashboard worden ontsloten. Het is voor “BOSOS” beheerder mogelijk om aangewezen gebruikers te markeren als beheerders namens de klant.

3. 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.

3.1 Eisen aan het inloggen

Wachtwoorden:

- Wachtwoorden worden gecodeerd opgeslagen in de database. Mocht een hacker ooit binnen komen dan kan hij geen wachtwoorden achterhalen van gebruikers. Beheerders en gebruikers kunnen daar vervolgens een persoonlijk wachtwoord van maken.
- Een nieuw wachtwoord opvragen kan door het ingeven van een e-mailadres in de hiertoe bestemde functie. Deze is te benaderen via het inlogscherf. Indien het ingevoerde e-mailadres in de applicatie bekend is, zal naar dit e-mailadres een mail worden gestuurd met een link. Via deze link kan een (nieuw) wachtwoord worden ingegeven.
- Een nieuw wachtwoord moet bestaan uit totaal minimaal 8 tekens waarvan:
 - minimaal 1 hoofdletter is
 - minimaal 1 kleine letter is
 - minimaal 1 cijfer is
 - minimaal 1 vreemd teken is (\$%&*#@# enz)
 - het wachtwoord mag geen spaties bevatten.
 - het wachtwoord mag niet het zelfde zijn als de Gebruikersnaam.

- Een beheerder heeft een bij voorkeur een organisatie gebonden e-mailadres. De beheerder is verantwoordelijk voor de e-mailadressen die worden ingevoerd. Bij voorkeur zijn de e-mailadressen van andere gebruikers ook organisatie gebonden en wordt geen gebruik gemaakt van hotmail en gmail of enig ander privé mailadres.
- Er wordt een dringend beroep gedaan aan alle gebruikers hun inloggegevens niet af te geven aan andere gebruiker. Iedere gebruiker moet apart worden ingevoerd en "BOSOS" en kan vervolgens eigen inloggegevens opvragen.
- Er wordt een dringend beroep op de gebruikers gedaan om voor het uitwisselen of bespreken van leerling gegevens alleen gebruik te maken van de e-mailfunctie die in "BOSOS" is opgenomen en niet via andere e-mail kanalen.

3.2 Eisen aan de verbinding

- Voor "BOSOS" wordt gebruik gemaakt van een beveiligde verbinding (https)
- De Onderwijsinstelling is verantwoordelijk voor een adequate bescherming middels antivirusprogramma's en firewall

3.3 Eisen aan opslag en back up

- Binnen de "BOSOS" applicatie worden alle data opgeslagen in een database. De gegevens in de database zijn vergrendeld.
- Aangeleverde bestanden worden 30 dagen bewaard.
- De servers zijn op de volgende manier beveiligd door middel van:
 - antivirusprogramma's;
 - software update's;
 - automatische back up's;
 - aparte afgesloten ruimte;
 - alleen binnen Nederland;
 - toegang alleen door geautoriseerd personeel.
- **Back-ups** maken het mogelijk om gegevens tot drie maanden lang terug in de tijd te herstellen. Elke drie uur wordt een back-up gemaakt van de databases. Database back-ups zijn tot drie maanden opvraagbaar. Dit gaat als volgt: de 3-uurse back-ups worden 4 dagen lang bewaard. Na deze vier dagen worden van al de 3-uurse back-ups er 1 per dag bewaard gedurende 10 dagen. Na deze 10 dagen worden 11 weken lang wekelijkse back-ups bewaard. Back-ups worden gemaakt van een secundaire replicatie server.
- **Replicatie:** Live replicatie houdt in dat data bijna realtime worden weggeschreven van primaire fysieke database servers naar een secundaire server. Wanneer iets mis is met de primaire database server neemt de secundaire database server de taken transparant over om continuïteit van de applicatie te garanderen.

3.4 Eisen aan de (beveiliging) van de applicatie of software

- Alleen geautoriseerde personen kunnen met "BOSOS" werken.
- De software is zo opgebouwd dat per onderdeel gebruikers geautoriseerd kunnen worden.
- Voor de leerlingen vragenlijst wordt per leerling toegang verleend. Na het invullen ervan sluit de applicatie en moet de volgende leerling weer een wachtwoord invoeren. Zo kunnen de leerlingen niet bij de gegevens van andere leerlingen. Het is leerkrachten verboden hun inloggegevens aan de leerlingen te geven.
- Per licentie wordt een beheerder benoemd die anderen toegang kan geven tot de delen van het programma waar mee gewerkt wordt.
- De beheerder neemt die verantwoordelijkheid over van de Bewerker. Die kan wel worden ingeschakeld wanneer er problemen m.b.t. het beheer zijn.
- Door de Subbewerker wordt de werking van "BOSOS" gemonitord.
- Er wordt 1x per jaar een pen-test uitgevoerd op www.bososs.nl en www.bososs2tot4.nl. De scan wordt uitgevoerd met een actuele software versie van Netsparker-Community Edition. Huidige versie Netsparker: 4.1.2.0.

- De Broncode is eigendom van Netgemak en is uitsluitend toegankelijk voor de ontwikkelaars, applicatie- en systeembeheerders. De Broncode is in Nederland opgeslagen. In de broncode worden geen gegevens opgeslagen, data worden uitsluitend in de database opgeslagen.
- Incryptie zit in de versleuteling van de gegevens en dat is gewaarborgd door het gebruik van SSL certificaten (Https).
- Wachtwoorden worden gecodeerd opgeslagen.
- Alleen binnen een schooljaar kunnen de gegevens worden bewerkt. M.i.v. het nieuwe schooljaar worden de gegevens gearhiveerd. Die kunnen wel worden benaderd maar niet meer worden bewerkt.
- Wanneer er een wijziging is van leerling gegevens waardoor die leerling uitstroomt, dan kan Subbewerker die informatie weer bij elkaar brengen

Dataservers en hostomgeving

Het "BOSOS" systeem maakt gebruik van een geavanceerde hostingomgeving om de betrouwbaarheid te maximaliseren. Het systeem wordt redundant gehost, hiermee wordt het volgende bewerkstelligd:

- Load balancing: gebruikers worden transparant vanuit de server met de laagste bezetting geserveerd;
- Fail over: als een server uitvalt kan de continuïteit van het systeem worden gegarandeerd omdat de werking door een andere server wordt overgenomen.

Ook voor de database server is gekozen voor een redundant systeem. Data worden bijna realtime op meerdere fysieke database servers opgeslagen. Deze constructie garandeert dat:

- als een database server uitvalt er geen gegevens verloren gaan, zelfs niet de gegevens die nog niet in de back-up procedure veilig zijn gesteld;
- back-ups worden gemaakt van de secundaire server zodat men hierdoor geen performance hindernis ondervindt;
- data altijd op twee locaties is opgeslagen; als met de primaire database server problemen ontstaan zal de secundaire database de taken transparant worden overgenomen.

4. 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.

4.1 Vertrek medewerker

Wanneer een medewerker vertrekt worden de "BOSOS" wachtwoorden waartoe de medewerkers beschikking had gewijzigd.

4.2 Vernietigen hardware

Gegevensdragers van afgeschreven hardware worden door middel van datavernietiging software onbruikbaar gemaakt. De volgende algoritmen kunnen worden gebruikt om de gegevens onherstelbaar te maken:

nnsa - U.S. NNSA Policy Letter NAP-14.1-C

dod - U.S. DoD 5220.22-M

usarmy - U.S. Army AR380-19

bsi - German Center of Security in Information Technologies

gutmann - 35-pass algorithm from Peter Gutmann's 1996 paper

schneier - algorithm described in Bruce Schneier's Applied Cryptography (1996)

pfitzner7 - Roy Pfitzner's 7-random-pass method

pfitzner33 - Roy Pfitzner's 33-random-pass method

Beveiligingsincidenten en/of datalekken:

Voor de werkwijze rond datalekken of mededelingen n.a.v. beveiligingsincidenten, verwijzen wij naar artikel 8 van de bewerkersovereenkomst.

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: [Peuter-Kleuterpraktijk Ellen Voogt info@peuter-kleuterpraktijk.nl](mailto:info@peuter-kleuterpraktijk.nl)

De contactpersoon voor Verwerker is: [Ellen Voogt](#)

Informereren over Datalekken en/of incidenten met betrekking tot beveiliging

Met de Onderwijsinstelling worden afspraken gemaakt over de afhandeling ervan.

Die afspraken omvatten:

- de wijze waarop monitoring en identificatie van incidenten plaatsvindt;
- de wijze waarop informatie wordt gedeeld;
- op welke manier (via e-mail, telefoon);
- aan wie gericht (contactpersonen en contactgegevens);
- met wie kan (bij vervolgacties) contact worden opgenomen;
- 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);
- eventuele afspraken of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie [3.0](#) 1 april 2018 laatst bijgewerkt 1 mei 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>.