

Deze bewerkersovereenkomst bevat de volgende bijlagen:

Bijlage 1: Privacy bijsluiter

Bijlage 2: Technische en organisatorische maatregelen

Bewerkersovereenkomst

Webbased Sociaal-emotioneel volgsysteem “Op School”

De Onderwijspraktijk Harry Janssens onderschrijft de afspraken die zijn gemaakt in het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant). Dit Convenant is afgesloten tussen de PO-Raad, VO-raad en de brancheorganisaties van educatieve uitgeverij (GEU), distributeurs van leermiddelen (leden van sectie educatief van de Koninklijke Boekverkoopersbond) en digitale dienstverleners in het onderwijs-ICT (VDOD).

Deze bewerkersovereenkomst is overeenkomstig de Model Bewerkersovereenkomst die als bijlage is toegevoegd aan het Convenant. De uitgangspunten daarvan sluiten aan bij de bepalingen in het Convenant, de Wet bescherming persoonsgegevens (hierna: Wbp) en de uitgangspunten zoals de jurisprudentie en de toezichthouder de Autoriteit Persoonsgegevens deze in richtsnoeren en afspraken heeft aangegeven. In het Convenant is afgesproken dat Onderwijsinstellingen en Ketenpartijen dit model gebruiken bij het maken van afspraken.

Deze Model Bewerkersovereenkomst bevat twee bijlagen:

1. In de Privacy Bijsluiter (Bijlage 1) wordt een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en onder welke doeleinden deze verwerkingen vallen.
2. In de Technische en Organisatorische Maatregelen (Bijlage 2) wordt omschreven welke beveiligingsmaatregelen er zijn getroffen.

Inleiding:

De Onderwijspraktijk Harry Janssens is de ontwikkelaar en eigenaar van het sociaal emotioneel volgsysteem "Op School". De gegevens van de leerlingen worden uitsluitend verwerkt in opdracht van de scholen waarmee een contract is afgesloten. Er worden geen gegevens aan derden verstrekt.

Partijen:

1. De Onderwijsinstelling:

Naam School:
BRINnummer:
Adres:
Postcode en plaats
Rechtsgeldig vertegenwoordigd door:

en

2. De bewerker

Naam: VOF Onderwijspraktijk Harry Janssens
Straat: Weeshuisplein 17
Postcode: 3311 SX
Plaats: Dordrecht

Rechtsgeldig vertegenwoordigd door: H. Janssens, onderwijsadviseur en eigenaar van "Op School"

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

Overwegen het volgende:

1. De Onderwijsinstelling en de Onderwijspraktijk Harry Janssens zijn een overeenkomst aangegaan voor het gebruik van het door de Onderwijspraktijk Harry Janssens aangeboden sociaal emotioneel volgsysteem "Op School". De Onderwijspraktijk biedt de Onderwijsinstelling de mogelijkheid voor de leerlingen screenings uit te voeren en handelingsplannen te maken op het gebied van gedrag en werkhouding. Dit is vastgelegd in de Product- en Dienstenovereenkomst, hierna te noemen Overeenkomst "Op School", die wordt afgesloten tussen de Onderwijsinstelling en de Onderwijspraktijk Harry Janssens. Dat contract leidt ertoe dat de Onderwijsinstelling gegevens van leerlingen en gebruikers aanlevert die door de Onderwijspraktijk worden ingevoerd en bewerkt in "Op School".
2. Partijen wensen, mede gelet op het bepaalde in artikel 14 Wet bescherming persoonsgegevens, in deze Bewerkerovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Bewerkersovereenkomst wordt verstaan onder:

- a) Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;
- b) Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;
- c) Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
- d) Convenant: het *Convenant Digitale Onderwijsmiddelen en Privacy*;
- e) Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, Wbp;
- f) Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g) 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;
- h) School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerling volgsysteem;
- i) Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
- j) Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
- k) Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
- l) Subbewerker: de partij die door Bewerker wordt ingeschakeld als Bewerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst en de Product- en Dienstenovereenkomst;
- m) Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1. Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling verstrekt aan de Bewerker de opdracht tot Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst.

Artikel 3: Rolverdeling

1. De Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verantwoordelijke. Bewerker is bewerker in de zin van de Wbp. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Bewerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Bewerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Bewerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie moet de Onderwijsinstelling in staat stellen een keuze te maken met betrekking tot de aangeboden diensten als zodanig, en daarnaast een afzonderlijke keuze te maken voor eventueel aangeboden optionele diensten.
3. De in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, moeten in de Privacy Bijsluiter bij deze Bewerkersovereenkomst in begrijpelijke taal zijn beschreven, waarna de Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en).
4. De Onderwijsinstelling kan verplicht zijn de Verwerking van de Persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De Onderwijsinstelling onderzoekt of zij hiervan is vrijgesteld en doet melding bij de Autoriteit Persoonsgegevens indien zij hiertoe verplicht is.
5. Onderwijsinstelling en Bewerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de relevante privacywet- en regelgeving mogelijk te maken.

Artikel 4: Privacy convenant

Partijen onderschrijven de bepalingen in het Convenant Digitale Onderwijsmiddelen en Privacy-leermiddelen en toetsen.

Artikel 5: Gebruik Persoonsgegevens

1. Bewerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan. Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
2. Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst
3. Bewerker onthoudt zich van verstrekking van Persoonsgegeven aan een Derde, tenzij deze uitwisseling plaatsvindt in opdracht van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een op de Bewerker rustende wettelijke verplichting.
4. In geval van een wettelijke verplichting, verifieert Bewerker voorafgaande de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker. Daarnaast informeert Bewerker de Onderwijsinstelling – indien wettelijk toegestaan - onmiddellijk, zo mogelijk voorafgaand aan de verstrekking. Indien Bewerker wordt verzocht Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde Derde, zijnde een andere onderwijsinstelling, zal de Bewerker slechts tot die verstrekking overgaan nadat deze onderwijsinstelling zijn BRIN kenbaar heeft gemaakt.

5. Artikel 6: Geheimhouding

1. Bewerker zorgt er voor dat iedereen waaronder haar werknemers, vertegenwoordigers en/of Subbewerkers, die betrokken zijn bij de Verwerking van de Persoonsgegevens deze gegevens als vertrouwelijk behandelen. Bewerker bewerkstelligt dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.
2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Bewerker aan Onderwijsinstelling te verlenen diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 7: Beveiliging en controle

1. Bewerker zal, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Deze maatregelen zullen, met inachtneming van de stand van de techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.
2. De maatregelen zoals genoemd in artikel 7.1 omvatten in ieder geval:
 - a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkerovereenkomst worden verwerkt;
 - b. maatregelen om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;
 - c. 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;
 - d. een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.
3. Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, 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 technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud en de frequentie van de rapportages die Bewerker aan de Onderwijsinstelling oplevert over de beveiligingsmaatregelen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Onderwijsinstelling moet treffen.
5. De Bewerker stelt de Onderwijsinstelling in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Bewerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, een geldige certificering of een gelijkwaardig controle- of bewijsmiddel.

6. In aanvulling op artikel 7, lid 4 heeft de Onderwijsinstelling te allen tijde het recht om, in overleg met de Bewerker en met inachtneming van een redelijke termijn, op eigen kosten, de door Bewerker genomen technische en organisatorische beveiligingsmaatregelen te laten toetsen door een onafhankelijke Register EDP auditor. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Bewerker in te schakelen gecertificeerde en onafhankelijke auditor die een derden-verklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

Definitie: een beveiligingsincident (datalek) is een gebeurtenis waarbij mogelijk de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of in gevaar kan komen.

1. Bewerker heeft een passend beleid voor de omgang met Datalekken.

Zodra een medewerker van "Op School" vermoedt dat er een beveiligingsincident heeft plaatsgevonden of er een melding wordt gedaan door een klant, wordt de volgende informatie verzameld:

- Datum en tijd van het vermoeden/incident
- Is het vaker voorgekomen? Indien ja, hoe vaak?
- Wat zijn de betrokken systemen en eventueel IPadressen?
- Welke URL'S zijn erbij betrokken?
- Wat zijn de foutmeldingen?
- Eventuele logfiles?

Deze informatie wordt doorgegeven aan de technische collega van dienst via het e-mailadres support@op-school.nl. De collega van deze afdeling trekt alle sporen na en trekt uit de resultaten van dat onderzoek zijn conclusies.

2. Indien Onderwijsinstelling dan wel Bewerker een Datalek vaststelt, dan zal deze de andere Partij onverwijld informeren. Bewerker verstrekt ingeval van een Datalek alle relevante informatie aan Verantwoordelijke met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Bewerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen. Aanvullend informeren Partijen elkaar onverwijld indien blijkt dat de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van Betrokken zoals bedoeld in artikel 34a, lid 2, Wbp.
3. Bewerker stelt bij een Datalek de Verantwoordelijke in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Bewerker dient hierbij aansluiting te zoeken bij de bestaande processen die Verantwoordelijke 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 Wbp of andere regelgeving betreffende de Verwerking van de Persoonsgegevens, te voorkomen of te beperken.
In alle gevallen zullen de wachtwoorden van medewerkers en gebruikers worden gewijzigd.
4. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. Partijen kunnen in onderling overleg bepalen of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten. Op verzoek van de Onderwijsinstelling kan Bewerker Onderwijsinstelling hierbij bijstaan en adviseren. De Onderwijsinstelling zal de Betrokkenen, indien wettelijk vereist, informeren over een dergelijke inbreuk. 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.

5. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

1. Een klacht of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door de Bewerker onverwijld doorgestuurd naar de Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
2. Bewerker verleent Onderwijsinstelling – voor zover redelijkerwijs mogelijk - volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Partijen zullen te goeder trouw overleggen over de redelijke verdeling van de eventuele kosten die hiermee gemoeid zijn.

Artikel 10: Verwerking buiten de Europese Economische Ruimte

Dit artikel is niet van toepassing op de Onderwijspraktijk Harry Janssens.
Alle gegevens staan op servers in Nederland.

Artikel 11: Inschakeling Subbewerker

1. Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.
2. Bewerker verplicht iedere Subbewerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na te leven met betrekking tot de Verwerking van Persoonsgegevens welke verplichtingen en maatregelen minimaal dienen te voldoen aan het bepaalde in deze Bewerkersovereenkomst.
3. Bewerker verplicht iedere Subbewerker contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Bewerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Bewerker. Bewerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen. Wanneer de Onderwijsinstelling de licentie overeenkomst met Bewerker opzegt, wordt die opzegging schriftelijk bevestigd. Daarin staat dat de toegang tot “Op School” gegarandeerd is tot 1 augustus van het betreffende kalenderjaar. Van de relevante documenten die de Onderwijsinstelling wil bewaren, kunnen PDF-bestanden worden gemaakt. Na 1 augustus zijn de gegevens niet meer toegankelijk voor de gebruikers. Tot 31 december van dat kalenderjaar blijven de gegevens nog beschikbaar voor het geval de Onderwijsinstelling er alsnog gebruik van wil maken. Na 1 januari van het daarop volgende kalenderjaar worden alle gegevens definitief uit “Op School” verwijderd. Mocht de Onderwijsinstelling langer toegang willen hebben tot de gegevens zonder ze verder te bewerken dan kan daar een aangepaste licentie overeenkomst voor worden afgesloten.
2. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
3. Bewerker zal alle Subbewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkersovereenkomst en zal waarborgen dat alle Subbewerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Tegenstrijdigheid en wijziging Bewerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Bewerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, zullen de bepalingen van deze Bewerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Bewerkersovereenkomst 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 Bewerkersovereenkomst 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, de doeleinden waaronder de Persoonsgegevens worden Verwerkt en het inschakelen van een (andere) Subbewerker. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Bewerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Bewerkersovereenkomst 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 14: Duur en beëindiging

1. De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Bewerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Bewerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Bewerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.

BIJLAGE 1: PRIVACY BIJSLUITER Sociaal Emotioneel Volgstelsel "Op School".

Scholen maken in toenemende mate gebruik van digitale toepassingen. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals leerlingen). Scholen moeten met Bewerker afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft scholen informatie over de dienstverlening die bewerkster verleent en welke persoonsgegevens de Bewerkster daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen wiens gegevens worden uitgewisseld.

Het gebruik van deze Privacy Bijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. In het kader van de herkenbaarheid is het wenselijk dat Bewerker zo veel mogelijk op uniforme wijze gebruik maken van de Privacy Bijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven.

A. Algemene informatie

Naam product en/of dienst	Sociaal Emotioneel Volgstelsel "Op School" Webbased
Naam Bewerkster en vestigingsgegevens	Onderwijspraktijk Harry Janssens Weeshuisplein 16-17, 3311 SX Dordrecht
Beknopte uitleg en werking product en dienst	Met "Op School" volgen leerkrachten de ontwikkeling van hun leerlingen op sociaal-emotioneel gebied (gedrag en werkhouding). Zij screenen de kinderen tweemaal per jaar en kunnen indien nodig handelingsplannen maken. De leerlingen vullen zelf leerling vragenlijsten in. 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.
Link naar leverancier en/of productpagina	www.op-school.nl
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. De specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen
Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.

1. De overeenkomst: de specifieke schoolgegevens van de deelnemer aan "Op School" worden ingevoerd: naam school, BRIN nummer, naam directeur, adres, telefoon en emailadres en de contactpersoon voor "Op School". De school kan kiezen voor het hele programma of voor het werken zonder leerlingen vragenlijsten of met alleen leerlingen vragenlijsten.
2. De gebruikers worden via een lijst aangeleverd en door Bewerkster 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 “Op School” met bijbehorende rechten. Een leerkracht kan alleen het dossier bewerken. De andere gebruikers niet. Die hebben inzagerecht.

3. Inhoud: via screenings wordt de ontwikkeling van de leerlingen gevolgd en wordt gekeken of er reden tot zorg is. Zo ja, dan kan de leerkracht een handelingsplan 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. De leerlingenlijst met smiley's wordt door de leerling zelf ingevuld. Dat is zodanig beveiligd dat de leerling alleen bij de eigen lijst kan en niet bij de andere gegevens in “Op School”. De leerkracht heeft inzage en kan een rapportage maken van de groep om zo zicht te krijgen op wat de leerling er zelf van vindt.
4. Scholen die met Parnassys werken, kunnen gebruik maken van een koppeling waardoor leerlingen en groepen rechtstreeks uit Parnassys in “Op School” 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.
5. Scholen die met andere leerlingen administratie systemen werken leveren via de site www.op-school.nl hun leerlingen lijsten aan die vervolgens door Subbewerker worden ingevoerd.
6. Gebruikers worden via een nieuwsbrief op de hoogte gehouden van het aanbod van de Onderwijspraktijk Harry Janssens. Dit aanbod is gericht op het primaire leerproces van de onderwijsinstelling. Iedere gebruiker heeft de mogelijkheid zich af te melden voor de nieuwsbrief.
7. Belangrijke mededelingen die met “Op School” te maken hebben, worden op de voorpagina (zichtbaar na het inloggen), geplaatst.
8. Aan Harry Janssens 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.
9. 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.

C. Doeleinden voor het verwerken van gegevens

1. het toegang krijgen tot en in gebruik kunnen nemen van “Op School”
2. analyse en interpretatie van de screenings
3. bijhouden van persoonlijke gegevens (waaronder medische) van een leerling en de eventuele gevolgen daarvan voor de sociaal emotionele 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 “Op School” werkt op verzoek van de Onderwijsinstelling

9. tijdelijke gebruikers toevoegen zoals vakleerkrachten of remedial teachers
10. continuïteit en goede werking van “Op School” 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. De Categorieën Persoonsgegevens worden gebruikt voor:

1. Registratie van licentiehouders “Op School”: naam school, naam directeur, BRINnummer, adres, telefoongegevens, e-mailadres, contactpersoon
2. Registratie van gebruikers waaronder de beheerders met naam, geslacht, e-mailadres, gebruikersnaam en rechten.
3. Registratie van leerlingen met hun naam, geboortedatum en geslacht.
4. De gebruikers worden via een nieuwsbrief op de hoogte gehouden van het aanbod gericht op onderwerpen die voortvloeien uit “Op School”. Die gegevens worden niet verstrekt aan andere leveranciers of aan derden.

E. Algemene informatie over getroffen beveiligingsmaatregelen

Voor de genomen veiligheidsmaatregelen wordt kortheidshalve verwezen naar Bijlage 2 bij de Bewerkerovereenkomst.

F. Subbewerkers

1. Bewerker maakt voor “Op School” gebruik van de volgende Subbewerker: Internetbureau Netgemak, Stationsplein 69, 7551 CR Hengelo. Zij hebben “Op School” technisch ontwikkeld en doen de hosting van het programma. Zij verzorgen het onderhoud van het programma, voeren in opdracht van de Onderwijspraktijk Harry Janssens 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 “Op School”. Tevens zijn zij contactpersoon voor de koppeling van “Op School” met Parnassys. Met Netgemak is een subbewerkerovereenkomst afgesloten
2. 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.

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiters of de werking van dit product of deze dienst, kunt u terecht bij: info@op-school.nl of info@onderwijspraktijk.nl, telefoon 078-6919160.

H. Versie van dit document

November 2016

Deze privacy bijsluiters maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-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://ww.privacyconvenant.nl>.

BIJLAGE 2: Technische en organisatorische beveiligingsmaatregelen voor “Op School”

1. Inleiding:

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkerovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens. Hier volgt een omschrijving van de maatregelen zoals bedoeld in artikel 7.2 van de Bewerkerovereenkomst

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.

2. 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.

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.

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

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

3.1 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 Onderwijspraktijk Harry Janssens als beheerder van “Op School”. 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 Onderwijspraktijk Harry Janssens vervult tevens de helpdeskfunctie, pr-activiteiten en facturering.
- Harry Janssens in zijn rol als onderwijsadviseur. Hij 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 “Op School” beheerders hebben de machtigingen om te bepalen welke gegevens via het dashboard worden ontsloten. Het is voor “Op School” beheerder mogelijk om aangewezen gebruikers te markeren als beheerders namens de klant.

4. 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.

4.1 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 inlogscherm. 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 "Op School" 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 "Op School" is opgenomen en niet via andere e-mail kanalen.

4.2 Eisen aan de verbinding

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

4.3 Eisen aan opslag en back up

- Binnen de "Op School" 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.

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

- Alleen geautoriseerde personen kunnen met "Op School" 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 "Op School" gemonitord.
- Er wordt 1x per jaar een pen-test uitgevoerd op www.op-school.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 gearchiveerd. 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

4.5 Dataservers en hostomgeving

Het "Op School" 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 secunsaire 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.

5. 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.

5.1 Vertrek medewerker

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

5.2 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

6. Rapportage

- 6.1 Mochten er technische en organisatorische maatregelen getroffen zijn die afwijken van de in dit document opgenomen beschrijvingen of die getroffen zijn naar aanleiding van een beveiligingsincident, dan zal de directie en contactpersoon van “Op School” van de Onderwijsinstelling daarvan schriftelijk op de hoogte worden gebracht.
- 6.2 Voor de werkwijze rond datalekken of mededelingen n.a.v. beveiligingsincidenten, verwijzen wij naar artikel 8 van de bewerkersovereenkomst. 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

November 2016