

Verwerkersovereenkomst 3.0 voor KIIJK! in de BSO

Inleiding

PO-Raad, VO-raad, MBO 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) hebben een convenant gesloten om ervoor te zorgen dat de privacy van gebruikers van digitale leermiddelen en datalekken is gewaarborgd. Bazalt onderschrijft de afspraken die in het Convenant Digitale Onderwijsmiddelen en Privacy, (hierna: Convenant) zijn gemaakt.

Deze verwerkersovereenkomst is gebaseerd op de verwerkersovereenkomst zoals die is opgenomen in het convenant. In het Convenant is afgesproken dat Onderwijsinstellingen en Ketenpartijen dit model gebruiken bij het maken van afspraken. Afwijkingen van het model worden schriftelijk gemotiveerd.

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 Privacybijsluiter (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.

Verwerkersovereenkomst:

Partijen:

- 1 Het bevoegd gezag van school, kinderopvangorganisatie, peuterspeelzaal of voorschool die met Bazalt een licentieovereenkomst heeft afgesloten voor het gebruik van KIIK! in de BSO, hierna te noemen: **“Onderwijsinstelling”**¹

en

- 2 Stichting Bazalt Groep, gevestigd en kantoorhoudende te:
Zandvoortselaan 146, 2554 EM, Den Haag
te dezen rechtsgeldig vertegenwoordigd door Annemarie Kaptein, Bestuurder van de Bazalt Groep, hierna te noemen: **“Verwerker”**

hierna gezamenlijk te noemen: **“Partijen”**, of afzonderlijk: **“Partij”**

Overwegen het volgende:

- a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij de onderwijsinstelling van Bazalt het programma KIIK! in de BSO ter beschikking gesteld krijgt om als digitaal onderwijsmiddel te gebruiken, de Product- en Diensten overeenkomst. Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
- b. Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

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;

¹ Onder ‘Onderwijsinstelling’ wordt dus ook verstaan: aanbieder van kinderopvang, peuterspeelzaal of voorschool.

- f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerling informatiemiddelen;
- 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 de kinderopvang, 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 leerlingvolgsysteem;
- s. Standaard attributenset: 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 omfattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.
 - w. Met KIIK! in de BSO wordt de webbased KIIK! in de BSO Registratie applicatie bedoeld.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

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

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.
3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Onderwijsinstelling in Bijlage 1 over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in Bijlage 1 opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en) en de uitvoering van de bijbehorende Verwerkingen.

4. De Onderwijsinstelling neemt de in lid 2 van dit artikel genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten² 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 Privacybijsluiter bij deze Verwerkersovereenkomst.
3. De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de Verwerkersverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt.
4. Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.
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 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.

² Zie voor een voorbeeld de Aanpak IBP bij <https://kn.nu/IBPonderwijs>

Artikel 6: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt ervoor dat eenieder 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. voorzover 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 ervoor 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 Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.
 - b. De auditor verstrekt het auditrapport alleen aan Partijen.
 - c. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
 - d. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
 - e. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken

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

Artikel 9: Bijstand

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

Voor gezien en akkoord.

Verwerker,

Stichting Bazaltgroep

A.J. Kaptein
Bestuurder Bazalt Groep
26 juli 2021

Bijlage 1: Privacybijsluitter

Bijlage 2: Beveiligingsbijlage

BIJLAGE 1 Privacybijsluiters KIJK! in de BSO (Digitaal onderwijsmiddel)

Inleiding

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 verwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.

Het uitvoeren van een Data Protection Impact Assessment (DPIA) wordt door de Bazalt Groep gedaan. Deze zal niet openbaar gemaakt worden.

A. Algemene informatie

Naam product en/of dienst	KIJK! in de BSO
Naam Verwerker en Vestigingsgegevens	Bazalt Groep Zandvoortselaan 146 2554 EM Den Haag
Beknopte uitleg en werking product en dienst	KIJK! in de BSO bestaat uit de digitale applicatie die bij de uitgave <i>KIJK! voor de BSO</i> hoort. KIJK! in de BSO is een instrument waarmee je op de BSO de betrokkenheid van kinderen, hun welbevinden en aspecten van sociaal competent gedrag observeert en registreert. Het helpt je om op een systematische wijze zicht te krijgen op de sociaal-emotionele ontwikkeling. De gegevens die je verzamelt zijn afkomstig uit twee bronnen: de pedagogisch medewerker en (vanaf dat het ongeveer 9 jaar oud is) het kind. Door deze twee bronnen bij elkaar te brengen, ontstaat een nauwkeurig en betrouwbaar beeld. Op basis van deze informatie is het mogelijk om in

	te spelen op de ontwikkelingsbehoeften en ontwikkelingsmogelijkheden van het kind. Alle kinderen van een kinderopvang of school zijn ingevoerd in het systeem, met voornaam, tussenvoegsel, achternaam, geslacht, geboortedatum, dagdelen per week. Eventueel zijn bijzonderheden in te voegen. Twee keer per jaar (gemiddeld) wordt de ontwikkeling van ieder kind geregistreerd.
Link naar uitgever en/of productpagina's	www.kijkindebso.nl www.bazalt.nl https://bazalt.nl/thema/jonge-kind/kijk/licenties.bazalt.nl
Doelgroep	Kinderopvang, voorscholen en scholen PO en besturen en aanbieders van buitenschoolse opvang (BSO).
Gebruikers	Medewerkers kinderopvang, kwaliteitsmedewerkers, pedagogisch coaches,

B. Omschrijving specifieke diensten

De Verwerking van Persoonsgegevens vindt plaats ten behoeve van:

- a. Licentie: het in gebruik kunnen nemen van het Digitale Onderwijsmiddel. Hiertoe worden van de licentiehouder naam, adres en emailadres geregistreerd.
- b. Toegang: het verkrijgen van toegang tot het aangeboden Digitale Onderwijsmiddel, waaronder de identificatie en autorisatie. Hiertoe worden van de beheerders en gebruikers hun voornaam, achternaam, geslacht en emailadres geregistreerd. De beheerders maken zelf wachtwoorden aan, die een domeinnaam van de organisatie hebben. Om privacy redenen zijn de domeinnamen zoals Hotmail en Gmail uitgesloten voor beheerders. Wachtwoorden zijn, ook om privacy redenen, niet zichtbaar voor de Verwerker en worden ook niet opgeslagen.
- c. Inhoud: met het digitale onderwijsmiddel wordt van kinderen/leerlingen de ontwikkeling geregistreerd. Hiertoe vindt opslag plaats van gegevens van de ontwikkeling van individuele kinderen en van alle kinderen samen in één groep.
- d. Data kunnen, volledig geanonimiseerd, gebruikt worden ten behoeve van wetenschappelijk en statisch onderzoek met als doel continu verbeteren van het product/de dienst.

De volgende groepen van medewerkers hebben toegang tot de software en de daarin opgeslagen persoonsgegevens:

- Medewerkers Bazalt:
 - a. *Medewerker Marketing:*
deze heeft inzage in alle administratieve gegevens van gebruikers ten behoeve van communicatie met gebruikers via het communicatiescherm. Zij kan niet bij ingevoerde kind gegevens.
 - b. *Secretariaat/Managementassistenten Bazalt Educatieve Uitgaven:*
zij hebben inzage in alle administratieve gegevens van gebruikers ten behoeve van klantenservice (hulp bij vragen, aanpassen licentie) en administratie (beheer klantgegevens, facturering). Zij kunnen niet bij ingevoerde kind gegevens.
 - c. *Onderwijsadviseurs, verantwoordelijk voor KIIK! in de BSO!:*
deze heeft inzage in gegevens ten behoeve van klantadvies bij inhoudelijke vragen. Indien de vraag dat nodig maakt, kan ook gewerkt worden met ingevoerde kind gegevens.

- Medewerkers Estrategy: Medewerkers bij Estrategy die de KIIK! software ontwikkelen, updaten en testen hebben ten behoeve van de helpdeskfunctie voor zowel Bazalt als voor gebruikers inzage in alle gegevens, inclusief kind gegevens.

Handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

- Bazalt Administrator ('Bazalt admin'): kan persoonsgegevens van gebruikers (klanten) inzien en wijzigen ten behoeve van klantenservice en administratie.
- Helpdesk: kan na expliciete toestemming van gebruiker meekijken in het beeldscherm van deze gebruiker.
- Administrator ('EstrategyAdmin'): kan bij alle facetten van het programma en kan op afstand hulp bieden.
- Software gericht: ontwikkelen, updaten en testen van het programma.

Koppelingen met andere programma's zijn er niet.

C. Doeleinden voor het verwerken van de gegevens.

KIIK! in de BSO is een School- en Leerling informatiemiddel. De verwerking van persoonsgegevens met behulp van KIIK! in de BSO vindt plaats ten behoeve van het bijhouden van ontwikkelingen van een kind en de gevolgen daarvan voor het volgen van onderwijs of vervolg aanbod;

D. Categorieën en soorten persoonsgegevens en classificatie

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:

- a. Van licentiehouders wordt geregistreerd: naam (voornaam, tussenvoegsel en achternaam), adres, emailadres;
- b. Van beheerders wordt geregistreerd: naam (voornaam, tussenvoegsel en achternaam), geslacht, emailadres;
- c. Van leerlingen wordt geregistreerd: naam (voornaam, tussenvoegsel en achternaam), geslacht, geboortedatum, dagdelen per week, (Eventueel zijn bijzonderheden in te voegen), observaties t.a.v. de ontwikkeling, registratie van de ontwikkeling. Deze laatste twee worden door de gebruiker toegevoegd; op de inhoud(skeuze) heeft Bazalt geen invloed of controle.

Classificatie

Voor de classificatie wordt uitgegaan van een 4 puntenschaal

- Beschikbaarheid: 2. Het is noodzakelijk dat het programma werkt als het gebruikt wordt. Enige mate van uitval heeft geen serieuze of essentiële schade tot gevolg
- Integriteit: 4. Fouten worden niet getolereerd.
- Vertrouwelijkheid: 3. Alleen beschikbaar voor een beperkte groep gebruikers.

In bijlage 2 worden de beveiligingsmaatregelen beschreven die hierop zijn afgestemd.

Bewaartermijnen:

Gegevens die niet meer worden gebruikt, worden door de verantwoordelijke beheerder van de onderwijsinstelling en kinderopvang in het archief van het programma gearchiveerd zodat ze op een later moment kunnen worden geraadpleegd. Gegevens worden tot 2 jaar na het verlaten van de BSO bewaard, tenzij de verantwoordelijk beheerder van de kinderopvang/onderwijsinstelling dit anders instelt. Indien de licentie wordt opgezegd door onderwijsinstelling wordt het account na 3 maanden verwijderd uit het systeem.

E. Opslag Verwerking Persoonsgegevens

Voor de genomen veiligheidsmaatregelen wordt korthedshalve verwezen naar Bijlage 2 bij de Verwerkersovereenkomst.

- Bewerker bewaart alle Persoonsgegevens die in KIIK! in de BSO worden ingevoerd op een server die alleen wordt gebruikt voor Bazalt-webapplicaties. Derden hebben geen toegang tot deze server en de daarop opgeslagen data.
- Land van opslag en verwerking van de persoonsgegevens: Nederland

F. Subverwerkers

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

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

a. Estrategy, Westsingel 98, 4461 DN Goes

Estrategy is de bouwer van de KIIK! in de BSO. applicaties. Deze subverwerker verzorgt het onderhoud van het programma, voert aanpassingen en updates uit (op aangeven van Bazalt) en verzorgt de helpdeskfunctie voor klanten met technische vragen. Om deze taken te kunnen uitvoeren heeft Estrategy de bevoegdheid van een administrator. Een administrator kan bij alle onderdelen van het programma.

Met deze Subverwerker is een Subverwerkersovereenkomst afgesloten. De Subverwerker is daarmee gebonden aan geheimhoudingsplicht omtrent Persoonsgegevens.

b. Uniserver, Robijnstraat 3, 1812 RB Alkmaar

Uniserver is de beheerder van de server die staat in een afgesloten ruimte. Naast motoring van de server wordt periodiek beheer op uitgevoerd (bijvoorbeeld het installeren van updates). UniServer heeft geen directe toegang tot de gegevens, omdat deze versleuteld zijn opgeslagen.

G . Contactgegevens

Voor vragen of opmerkingen over deze bijsluiters of de werking van dit product of deze dienst, kunt u terecht bij Bazalt: info@bazalt.nl of 088-55 70 500

H. Versie van dit document

Versie 1.0, 26 juli 2021

Deze Privacy Bijsluiters maakt deel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-e en vDOD), het ministerie van OCW. Meer informatie hierover vindt u hier: www.privacyconvenant.nl

Overzicht gegevens en bewerkingen

Soort verwerking	Toelichting	Categorie gegevens	Gegevens	Doelinden	Toegang verwerker (Bazalt)
Licentie afsluiten	Verantwoordelijke ('klant') sluit een overeenkomst af met Bazalt, verstrekt de benodigde gegevens en wordt licentiehouders	NAW	Voornaam Achternaam Adres e-mailadres	Verantwoordelijke in staat stellen het programma te kunnen gebruiken.	Klantenservice Bazalt (= Bazalt admin)
Toegang verlenen	De verantwoordelijke stelt een beheerder aan die gebruikers aanmaakt en/of groepen kinderen toevoegt of aanmaakt.	NAW	Voornaam Achternaam Geslacht e-mailadres	Beheerder in staat stellen met het programma te kunnen werken.	Klantenservice Bazalt (= Bazalt admin)
Inhoudelijke ondersteuning	De verantwoordelijke gebruiker voert kindgegevens in zodat vervolgens per kind observatiegegevens m.b.t. ontwikkelingsgebieden kunnen worden geregistreerd.	NAW	Voornaam, Tussenvoegsel Achternaam Geslacht Thuisstaat Geboortedatum VVE-leerling (ja/nee) Dagdelen per week Datum plaatsing groep (eventueel bijzonderheden)	Identificeren kind	Onderwijsadviseur, inhoudelijk verantwoordelijke (= admin) t.b.v. helpdesk functie
		Ontwikkelingsvoortgang	Registraties in de vorm van basisgegevens en op	Inzicht hebben in de SEO ontwikkeling van een	Applicatie

	<p>Per kind en per groep kan een overzicht worden verkregen.</p> <p>Verwerker werkt <u>niet</u> met de gegevens. Toegang kan nodig zijn voor inhoudelijke vragen.</p>		<p> sociaal emotionele domeinen</p>	<p> kind om op basis daarvan het juiste vervolgaanbod te kunnen bieden.</p>	<p>Tot deze gegevens heeft alleen de beheerder rechtstreeks toegang.</p>
<p>Technische ondersteuning</p>	<p>Wordt door sub-verwerker verleent. Ook de sub-verwerker werkt <u>niet</u> met de gegevens. Toegang kan plaatsvinden in geval van technische problemen.</p>	<p>NAW</p> <p>Ontwikkelingsvoorgang</p>	<p>Voornaam Achternaam Geboortedatum</p> <p>Registraties van basisgegevens en op sociaal emotionele domeinen.</p>	<p>Technische helpdeskfunctie (t.b.v. verwerker = Bazalt medewerker)</p>	<p>Medewerker EStrategy</p>

BIJLAGE 2: Beveiligingsbijlage KIJK! in de BSO

Inleiding

In bijlage 1 wordt een overzicht gegeven van de persoonsgegevens die worden verwerkt met de plaats waar ze worden opgeslagen. Zoals opgenomen in artikel 7 van deze verwerkersovereenkomst treft verwerker passende technische en organisatorische maatregelen om de Persoonsgegevens te beschermen tegen verlies, onrechtmatige verwerking of onrechtmatige toegang. Een en ander rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging van deze maatregelen.

De maatregelen worden in deze bijlage beschreven.

A. Algemene informatie over getroffen beveiligingsmaatregelen

De Educatieve uitgeverij van Bazalt maakt deel uit van de Bazalt Groep.

De Bazalt Groep hecht veel belang aan het juiste gebruik van (persoons)gegevens. Daarvoor is beleid geformuleerd dat actief wordt uitgedragen en zijn gegevensstromen in kaart gebracht, zodat maatregelen kunnen worden genomen om te zorgen voor:

1. Beschikbaarheid van gegevens op het juiste moment.
2. Integriteit van gegevens: het waarborgen van de correctheid en de volledigheid van informatie en verwerking waardoor informatie met de werkelijkheid in overeenstemming is en niets ten onrechte is achtergehouden of verdwenen.
3. Vertrouwelijkheid van gegevens: het waarborgen dat informatie alleen beschikbaar is voor degenen die hiertoe geautoriseerd zijn.

(persoons)Gegevens worden alleen gedurende de periode van de werkzaamheden plus de wettelijke / vastgelegde bewaartermijnen, dus tijdelijk, opgeslagen. Aan de hand van een risico matrix wordt bepaald welke mate van gegevens beveiliging van toepassing is.

De Raad van Bestuur van De Bazalt Groep is verantwoordelijk voor het beveiligingsbeleid. Het beleid met betrekking tot beveiliging is geïntegreerd in het kwaliteitsbeleid van de Bazalt Groep wat verankerd is in de eisen van ISO 9001:2015 om te voldoen aan wettelijke regelingen. In dit kader is het voldoen aan de eisen van de AVG. Zo is in het kwaliteitssysteem een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten en worden Informatiebeveiligingsincidenten benut voor optimalisatie van het informatiebeveiligingsbeleid.

De getroffen beveiligingsmaatregelen worden met het kwaliteitssysteem door de kennismanager gecheckt en bewaakt; het zorgen voor veiligheid en integriteit met betrekking tot de informatie op zich, is de verantwoordelijkheid van de betreffende managers en de medewerkers die met de gegevens werken. Werken aan kwaliteit is geïntegreerd in het handelen van alle dag.

B. Maatregelen om persoonsgegevens te beschermen tegen verlies of wijziging en tegen onbevoegde of onrechtmatige verwerking, toegang of openbaarmaking.

- *De beschikbaarheid en continuïteit van de programma's is gewaarborgd door:*
 - Periodieke updates
 - Noodstroomvoorziening
 - Juridische vormgeving Bazalt binnen de Bazalt Groep
 - De applicaties draaien op de server van Uniserver.
 - Er is geen sprake van Escrow. Wel is aangesloten bij ICTWaarborg. ICTWaarborg zorgt er in *worst case* situatie voor dat er binnen het netwerk wordt gezocht naar een partner die de zaken kan overnemen. (Meer informatie is te lezen op de website van ICTWaarborg: <https://www.ictwaarborg.nl/>)
 - Elke nacht wordt door Estrategy een back up van de database gemaakt, die 's morgens intern naar de server wordt overgezet.

- *Maatregelen die er voor zorgen dat de integriteit wordt gewaarborgd*

De programma's zijn zodanig opgezet dat gegevens niet automatisch veranderd kunnen worden. Tussentijds worden stappen opgeslagen. Op essentiële punten kunnen alleen de administrator en de webbouwer veranderingen aanbrengen.

- *Maatregelen die ervoor zorgen dat de vertrouwelijkheid van de gegevens gewaarborgd is:*
 - uitsluitend bevoegd personeel toegang heeft tot de persoonsgegevens
 - Autorisatiebeleid
 - De Bazalt Groep hanteert een autorisatiebeleid om ervoor te zorgen dat medewerkers alleen toegang hebben tot Persoonsgegevens voor zover dat nodig is om hun werkzaamheden uit te voeren.
 - Eisen aan de medewerker
 - Medewerkers van de Bazalt Groep zijn voor alles gebonden aan de integriteits- en geheimhoudingscode die richtlijnen geeft voor nauwgezet en zorgvuldig handelen uitgaand van de belangen van alle betrokkenen.
 - Hoewel er afspraken zijn gemaakt over de omgang met (vertrouwelijke) informatie en technische en organisatorische maatregelen zijn getroffen, is de Bazalt Groep er zich van bewust dat je niet alles kunt regelen of overal afspraken over kunt maken. Medewerkers moeten automatisch 'weten' wat ze wel of niet mogen en kunnen doen met gegevens om de integriteit en de vertrouwelijkheid te waarborgen. Deze 'risico bewuste houding' hoort 'bij de bagage' van medewerkers. De Bazalt Groep stimuleert dit bewustzijn ten aanzien van privacy en informatiebeveiliging en checkt het gedrag jaarlijks onder andere in de audits in het kader van de ISO-certificering.
 - Met betrokken sub verwerkers zijn overeenkomsten afgesloten zodat de persoonsgegevens zijn beveiligd, niet veranderd kunnen worden en niet verloren kunnen gaan.

- Geheimhoudingsverklaring
 - Met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt
 - Van subverwerkers wordt verwacht dat zij een geheimhoudingsverklaring hebben getekend conform hun eigen (vereiste) beveiligingsbeleid. Dit beveiligingsbeleid wordt/is tevoren gecontroleerd en wordt jaarlijks getoetst.

- Technische en organisatorische maatregelen m.b.t. netwerk-, server- en applicatiebeveiliging en onderhoud:
 - De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Verkeersstromen worden gescheiden en er zijn maatregelen geïmplementeerd tegen misbruik en aanvallen. Te denken valt o.a. aan:
 - Antivirusprogramma's;
 - een firewall;
 - Automatische software updates;
 - Het periodiek installeren van de laatste (beveiligings-)patches op basis van patchmanagement.
 - Automatische back-ups, die dagelijks worden gemaakt. Indien er problemen voordoen optreden, kan vanuit de back up de juiste informatie worden terug gehaald.
 - Een aparte afgesloten serverruimte die alleen toegankelijk is voor geautoriseerd personeel waaronder een netwerkbeheerder die het netwerk onderhoudt en problemen voorkomt en oplost;
 - Versleutelde gegevens in de diverse databases;
 - Het voorkomen en tijdig detecteren van aanvallen, inbraken of inbraakpogingen;
 - Het gebruiken van software waarbij per onderdeel gebruikers geautoriseerd kunnen worden en ook de handelingen die ze met de gegevens kunnen verrichten zijn geautoriseerd.
 - Op lokale werkstations en servers worden passende maatregelen genomen om te voorkomen dat kwaadaardige programmatuur of functionaliteit wordt geïnstalleerd. Datzelfde geldt voor telefoon, tablets zoals iPads en laptops. Te denken valt aan wachtwoordmanagement maar ook aan autorisatie m.b.t. installeren van programma's.
 - Op wachtwoorden worden cryptografische maatregelen (hashing) toegepast, van een kwaliteit die in de industrie over het algemeen als veilig wordt beschouwd, om deze gegevens veilig op te slaan. Er wordt voor inlogprocessen gebruik gemaakt van beveiligde / versleutelde verbindingen w.o. https (TLS-certificaten).
 - **Specifiek eisen aan het inloggen van KIJK! in de BSO:**
 - Een beheerder dient een organisatiegebonden emailadres te hebben. Adressen met de domeinnamen zoals hotmail en gmail zijn uitgesloten. Beheerder is verantwoordelijk voor de

emailadressen die worden uitgegeven. Ook hier geldt: geen andere dan organisatie-gebonden emailadressen;

- Wachtwoord moet telkens worden ingevoerd (wordt niet opgeslagen);
- Om de drie maanden moet het wachtwoord worden gewijzigd;
- Na drie keer foutief inloggen wordt het account geblokkeerd;
- Na 30 minuten zonder activiteit wordt automatisch uitgelogd;
- Wachtwoorden moeten voldoen aan de volgende eisen: minimaal 8 tot maximaal 128 karakters / minimaal 1 hoofdletter / minimaal 1 cijfer / minimaal 1 van deze symbolen (!@#\$%^&*()_-=+`~.,/?:;|)

○ **Eisen aan de gebruiker van KIJK! in de BSO:**

- De gebruiker is verantwoordelijk voor het gebruik van de software en de communicatie van de gegevens van de kinderen aan hun ouders/verzorgers.
- Vanuit zijn verantwoordelijkheid zorgt Bazalt voor een goede werking van de software en informatie die nodig is om dit te waarborgen. Daaronder vallen ook zaken die van de gebruiker vereist worden. Bazalt heeft deze zaken opgenomen in de Licentieovereenkomst.
- Van de gebruiker wordt verwacht dat hij zorgt voor adequate bescherming middels antivirusprogramma's en firewall.

○ **Eisen aan de (beveiliging) van KIJK! in de BSO:**

- Alleen geautoriseerde personen kunnen met de programma's werken. Per licentie wordt een beheerder benoemd die anderen toegang kan geven tot de delen van de software waarmee gewerkt moet worden.
- De software is zodanig opgebouwd dat per onderdeel gebruikers geautoriseerd kunnen worden.
- De beheerder kan het systeem zo inrichten dat je vooraf de IP adressen invoert van waaruit alleen maar ingelogd mag worden in het systeem. Hiermee kun je uitsluiten dat er vanuit ongewenste IP adressen wordt ingelogd.
- Deze beheerder neemt de verantwoordelijkheid van de Verwerker over. Dit is in de licentie overeenkomst geregeld.
- Vanuit Estrategy monitort een zogenaamde administrator ('admin') de werking van de programma's.

- De uitwisseling van persoonsgegevens, ook via e-mail, tussen de onderwijsinstelling en De Bazalt Groep vindt beveiligd, versleuteld en in pdf plaats.

C. Plaats/Land van opslag en Verwerking van de Persoonsgegevens

Verwerker zal geen persoonsgegevens van Verwerkingsverantwoordelijke doorgeven aan (een partij gevestigd in) een land dat door de Europese Unie niet is aangemerkt als een land waar privacy adequaat is beschermd, tenzij Bewerker met de betreffende partij een verwerkersovereenkomst heeft gesloten waarbij de relevante door de Europese Commissie beschikbaar gestelde modelclausules zijn opgenomen. Verwerking in de Verenigde Staten is niet toegestaan.

Voor alle gegevens geldt dat ze binnen de Europese ruimte worden opgeslagen. De servers van Uniserver staan in Nederland. De Bazalt Groep werkt met Office365, maar persoonsgegevens worden niet opgeslagen in de cloud van Microsoft.

D. Maatregelen voor opsporen van zwakke plekken en incidentenbeheer:

Analyseren van incidenten en problemen:

In het kader van de ISO certificering analyseert de Bazalt Groep ook de beveiliging van (persoons)gegevens en eventueel voorkomende incidenten. Het is de bedoeling tot structurele verbeteringen te komen.

Problemen oplossen en voorkomen

- Op basis van de analyse kan de verantwoordelijke bij incidenten geholpen worden het probleem van een incident of data lek bij de AP te melden.
- Daarnaast worden preventief informatie beveiligingschecks uitgevoerd en wordt het beveiligingsbeleid van derden jaarlijks gecheckt.
- Dit geldt ook voor technische apparatuur waarmee gewerkt wordt, zodat apparatuur tijdig kan worden vervangen en continuïteit en de opslag van gegevens blijvend gegarandeerd is.

Informereren over inbreuken (datalekken) met betrekking tot beveiliging

De Bazalt Groep monitort haar dienstverlening voortdurend en heeft de in deze bijlage opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatig toegang tot gegevens te voorkomen. Mocht er onverhoopt toch een inbreuk signaleerd worden, dan zal De Bazalt Groep zo spoedig mogelijk melding hiervan maken bij de betreffende Verwerkingsverantwoordelijke in de zin van de AVG. Om een en ander snel en volgens de regels mogelijk te maken is een meldpunt datalekken ingericht en een protocol / procedure datalekken opgesteld

De melding zal in ieder geval de volgende informatie bevatten:

- 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).

Of melding van een inbreuk bij de Autoriteit Persoonsgegevens en eventueel de betrokkenen vereist is, is aan de verwerkingsverantwoordelijke om te beslissen. De Bazalt Groep zal er alles aan doen om de Verwerkingsverantwoordelijke in staat te stellen de melding binnen de 72 uur te doen plaatsvinden

E. versie

De Bazalt Groep zal de inhoud van deze overeenkomst / bijlage van tijd tot tijd bijwerken. De meest actuele versie staat altijd op www.bazalt.nl/privacy.

Versie 1, Den Haag, 26 juli 2021