

Verwerkersovereenkomst Odin Onderwijs B.V. h.o.d.n. Heutink ICT

Deze Verwerkersovereenkomst is volledig identiek aan de Model Verwerkersovereenkomst 3.0 zoals tot stand gekomen binnen de Nederlandse onderwijssector en is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

heutink.ict

Heutink ICT is een handelsnaam van Odin Onderwijs B.V.

Partijen:

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

en

2. De besloten vennootschap Odin Onderwijs B.V., handelend onder de naam Heutink ICT, gevestigd en kantoorhoudende aan Expolaan 50, te (7556 BE) Hengelo, te dezen rechtsgeldig vertegenwoordigd door Rogier Borggreve (Algemeen Directeur), hierna te noemen: “Verwerker”

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

Overwegen het volgende:

- a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij Verwerker in opdracht van Onderwijsinstelling een onderwijscommunicatieplatform levert (‘de Product- en Dienstenovereenkomst’). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
- b. Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

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 toetgetreden Onderwijsinstelling of Leverancier;
- e. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
- f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g. Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
- h. Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst. Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);
- i. KetenID: 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 KetenID, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het KetenID wordt ook ECK iD genoemd;
- j. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;

- k. Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
- l. Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
- m. Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
- n. Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
- o. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;
- p. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
- q. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
- r. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem, studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerling volgsysteem;
- s. Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het KetenID gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);
- t. Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
- u. AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG).
- v. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen 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 verwerkingsactiviteiten¹ die onder hun verantwoordelijkheid plaatsvinden.
5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.
6. Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4: Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een in hoogste instantie gewezen rechterlijke uitspraak op grond waarvan Verwerker tot Verwerking, waaronder begrepen mogelijk verstrekking, verplicht is. 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

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

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

Artikel 6: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij betreft bij de Verwerking van Persoonsgegevens, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerkers, deze gegevens als vertrouwelijk behandelt. Verwerker waarborgt dat met de tot het Verwerken van de Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding zijn gebonden.
2. De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:
 - a. voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;
 - b. indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of
 - c. indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel een in hoogste instantie gewezen gerechtelijke uitspraak 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 gerechtelijke uitspraak, voor zover

daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker – tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.

4. Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 7: Beveiliging en controle

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

- d. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
- e. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken

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

Artikel 9 Bijstand

1. Verwerker verleent Onderwijsinstelling bijstand bij het doen nakomen van de op Onderwijsinstelling rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking – maar niet beperkt – tot:

- a. het – voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
 - b. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
 - c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortvloeiende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
 - d. Het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
 - e. Het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.
2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
 3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

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

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

werkersovereenkomst 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 hier toe 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, 6, 9 en 12.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,

Verwerker,

Naam:

Functie:

Datum:

Naam: Rogier Borggreve

Functie: Algemeen Directeur

Datum: 27 februari 2020

Bijlagen

Bijlage 1: Privacybijsluiters

Bijlage 2: Beveiligingsbijlage

Bijlage 3: Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA

Bijlage 4: Toelichting op maatregelen toetsingskader Certificeringsschema Informatiebeveiliging en Privacy ROSA

BIJLAGE 1: PRIVACYBIJSLUITER GEBRUIK ONDERWIJSCOMMUNICATIEPLATFORM KLASBORD

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.

A. Algemene informatie

Naam product en/of dienst	: Klasbord
Naam Verwerker en vestigingsgegevens	: Odin Onderwijs B.V., handelend onder de naam Heutink ICT (Expolaan 50, 7556 BE, Hengelo)
Link naar <u>leverancier</u> en/of productpagina	: https://klasbord.nl
Beknopte uitleg en werking product en dienst	:

Klasbord is een beveiligde afgeschermd communicatieplatform voor scholen. Middels een web-app en mobiele app kan vanuit de school contact worden gelegd met de ouders. De informatie, die kan bestaan uit tekst en/of een foto, kan binnen een gesloten groep worden gedeeld met de betrouwen. De informatie is alleen toegankelijk door in te loggen op het platform. Gebruikers creëren en beheren zelf een persoonlijk account, waar zij tenminste de volgende gegevens invoeren: naam, e-mailadres.

Doelgroep (zoals po/vo, onderbouw/bovenbouw)	: PO
Gebruikers	: Onderwijsdeelnemers, ouders/verzorgers, docenten.

B. Omschrijving specifieke diensten

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

Klasbord gedeelde gegevens			
Bij gebruik van Klasbord maak je gebruik van deze onderliggende verwerkingen:			
Onlosmakelijke verwerking			
Gegevens (* is verplicht)	Doel	Categorie	Bewaartermijn
Account Voornaam * Achternaam * E-mailadres * Profielfoto	A.5, B, C, D, E	1, 4, 11	Accounts worden na 2 jaar inactief te zijn geweest, automatisch middels e-mail op de hoogte gebracht en verwijderd indien geen actie wordt ondernomen. Gebruiker kan op elk moment zijn/haar account verwijderen.
Profiel volger Naam kind Relatie tot de groep/kind *	A.5	4	Profielgegevens gerelateerd aan de volger van een groep worden automatisch verwijderd wanneer de groep wordt verlaten of de groep in zijn geheel wordt verwijderd.
Groepsberichten Groepsberichten en -evenementen die tekst, bijlagen, beeldmateriaal en/of reacties van persoonlijke aard kunnen bevatten.	A.5	10	Groepsberichten worden automatisch verwijderd, inclusief reacties en bijlagen, wanneer de groep wordt verwijderd.

C. Doeleinden voor het verwerken van gegevens

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

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

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

- A.** de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:
 - ~~1) de indeling en aanpassing van roosters;~~
 - ~~2) de analyse en interpretatie van leerresultaten;~~
 - ~~3) het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;~~
 - ~~4) het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;~~

- 5) de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;
- ~~6) financieel beheer;~~
- ~~7) monitoring en verantwoording, ten behoeve van met name: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;~~
- ~~8) het behandelen van geschillen.~~
- ~~9) het uitwisselen van Persoonsgegevens met Derden, waaronder:

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

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

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

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

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

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

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

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

~~**i.** De uitvoering of toepassing van een andere wet~~

D. Categorieën en soorten persoonsgegevens

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

Categorie	Toelichting
1. Contactgegevens	naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens; Beperkte set = naam, e-mail, opleiding; Persoonlijke set = geboortedatum, geslacht;
2. Onderwijs-deelnemer-nummer	een administratienummer dat onderwijsdeelnemers identificeert
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
5. Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
7. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: <ul style="list-style-type: none"> • klas / leerjaar / ILT code • Examinering • Studievoortgang en/of Studietraject • Begeleiding onderwijsdeelnemers, inclusief handelingplan • Aanwezigheidsregistratie
8. Onderwijsorganisatie	gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
9. Financiën	gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, alsmede bankrekeningnummer van de betrokkene;
10. Beeldmateriaal	foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;
11. Docent, zorg-coördinator, intern begeleider, decaan, mentor	gegevens van docenten en begeleiders , voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;
12. Overige gegevens, te weten	andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet. Wel moet worden vermeld om welke gegevens het gaat.
13. BSN/PGN	
14. Keten ID (ECK ID)	unieke ID voor de 'educatieve contentketen'. Hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

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

Voor de bewaartermijnen van Persoonsgegevens, zie “**B. omschrijving van de specifieke diensten**”

E. Opslag Verwerking Persoonsgegevens:

Alle persoonsgegevens worden verwerkt door onze subverwerkers, zie “**F. Subverwerkers**”

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.

Klasbord App en Web-App		
Subverwerker & plaats	Functionaliteit	Verwerkte gegevens
Tilaa Amsterdam	Opslaan en authenticeren van gebruikers. Opslaan van foto's, video's en bestanden.	Accountgegevens, Groepsgesprekken, Beeldmateriaal
Sparkpost West-Europa	Versturen van e-mail meldingen.	Voornaam, achternaam, E-mailadres.
Drukkerij Formaat Helvoirt	Afdrukken en verzenden van Klasboeken	Naam, adres, Digitaal afdrukbestand met beeldmateriaal

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiters of de werking van dit product of deze dienst, kunt u terecht bij: Heutink ICT, Expolaan 50, 7556 BE, Hengelo. Heutink ICT is een handelsnaam van Odin Onderwijs B.V..

privacy@klasbord.nl

H. Versie

Versie 3.0 – laatste aanpassing 27 februari 2020

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

BIJLAGE 2: BEVEILIGINGSBIJLAGE

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

Minimale beveiligingsmaatregelen en aantoonbaarheid

Verwerker plaatst op deze plek in de bijlage een verklaring waaruit blijkt dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat ten minste:

- a. Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;
- b. Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;
 - i. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
 - ii. Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;
 - iii. Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Hierbij heeft Verwerker procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
 - iv. Verwerker zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
 - v. Verwerker heeft procedures voor 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 Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren;
 - vi. Verwerker heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
 - vii. Verwerker maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter)nationale beveiligingsnorm;
 - viii. Verwerker heeft maatregelen genomen 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.
- c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: support@klasbord.nl

De contactpersoon voor Verwerker is: _____

Informereren over Datalekken en/of incidenten met betrekking tot beveiliging

Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:

- 1) De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
- 2) De wijze waarop informatie wordt gedeeld:
 - a) Op welke manier (via e-mail, telefoon);
 - b) Aan wie gericht (contactpersonen en contactgegevens);
 - c) Met wie kan (bij vervolgacties) contact worden opgenomen.
- 3) Informatie die in ieder geval over een incident gedeeld moet worden
 - a) 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);
 - b) De oorzaak van het beveiligingsincident;
 - c) De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
 - d) Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
 - e) De omvang van de groep betrokkenen;
 - f) 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).
- 4) Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie 3.0 – laatste aanpassing 27 februari 2020

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

BIJLAGE 3: Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA

Deze bijlage is gebaseerd op de classificatie 2.01 binnen het certificeringsschema informatiebeveiliging en privacy ROSA: <https://www.edustandaard.nl/app/uploads/2018/06/3. Certificeringsschema classificatie.xlsx>

Beschikbaarheid				
Vragen	Motivatie	Laag	Mid-den	Hoog
<p>Wanneer moet de dienst beschikbaar zijn voor de gebruikers?</p> <ul style="list-style-type: none"> - Laag = regulier (bijvoorbeeld alleen kantooruren) - Midden = ruim (bijvoorbeeld 07:00 - 23:00 en/of ook in het weekend) - Hoog = altijd (bijvoorbeeld 24x7) 	<p>Het grote gebruik van Klasbord begint rond 8uur in de ochtend en eindigt rond 11uur in de avond.</p>		X	
<p>Wat is de langste periode dat de ict-toepassing niet beschikbaar mag zijn?</p> <ul style="list-style-type: none"> - Laag = maximaal enkele dagen - Midden = maximaal een aantal uur - Hoog = maximaal een aantal minuten 	<p>Het platform is vaak het enige communicatiemiddel naar de ouders toe. In het geval er een bericht of foto gedeeld dient te worden dient het platform hooguit enkele uren niet beschikbaar te zijn.</p>		X	
<p>Welke impact heeft uitval (de data, informatie of de ict-toepassing zijn niet beschikbaar)?</p> <ul style="list-style-type: none"> - Laag = geen - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan 	<p>Het delen of bekijken van een bericht en/of foto is tijdens een uitval niet mogelijk. Na de uitval kan dit weer worden voortgezet.</p>		X	
<p>Op hoeveel gebruikers/organisaties heeft uitval impact?</p> <ul style="list-style-type: none"> - Laag = bij uitval van de toepassing worden slechts enkele gebruikers/organisaties geraakt - Midden = bij uitval van de toepassing worden grote groepen gebruikers/organisaties geraakt - Hoog = bij uitval van de toepassing wordt een substantieel aandeel van de gebruikers/organisaties geraakt 	<p>Niet alle geregistreerde gebruikers maken dagelijks gebruik van het platform. Bij uitval zal dus een deel van deze gebruikers hinder ervaren.</p>		X	
<p>Zijn er contractuele verplichtingen voor de beschikbaarheid?</p> <ul style="list-style-type: none"> - Laag = nee - Midden = ja, er is een standaard SLA of er staan algemene beschikbaarheidseisen in het contract - Hoog = ja, er is een uitgebreide SLA afgedwongen inclusief eisen voor rapportage en responstijd voor incidenten 		X		

	<p>Wat is de verwachte belasting van de ict-toepassing?</p> <ul style="list-style-type: none">- Laag = weinig gelijktijdige gebruikers (honderden), weinig transacties (100 per uur), minder dan 1000 requests per seconde- Midden = gelijktijdige gebruikers (duizenden), normale hoeveelheid transacties (100-500 per uur), tussen 1000 en 2000 requests per seconde- Hoog = veel gelijktijdige gebruikers (vele duizenden), veel transacties (meer dan 500 per uur), meer dan 2000 requests per seconde	<p>Op het moment van schrijven wordt het platform dagelijks door gemiddeld 100.000 unieke gebruikers bezocht.</p>			
				X	
	B=	2			
	Omschrijving	Kenmerken			
Niveau 1:	Beschikbaarheid is onbelangrijk.	RTO*= 24-48 uur, afhankelijk van de categorie informatie			
Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.				
Niveau 2:	Beschikbaarheid is belangrijk.	RTO*= 8-24 uur, afhankelijk van de categorie informatie			
Midden	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.				
Niveau 3:	Beschikbaarheid is noodzakelijk.	RTO*= 1-8 uur, afhankelijk van de categorie informatie			
Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.				

* RPO is een kenmerk onder integriteit

Integriteit

Vragen	Motivatie	Laag	Midden	Hoog
<p>Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen?</p> <ul style="list-style-type: none"> - Laag = nee, de gegevens lenen zich niet voor fraude - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens 	<p>Er worden geen leerresultaten of financiële gegevens met betrekking tot de school verwerkt.</p>	X		
<p>Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten?</p> <ul style="list-style-type: none"> - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan 	<p>Bij een foutieve invoer of ongeautoriseerde verandering kan deze door een medewerker van de helpdesk worden aangepast. In het geval van een ongeautoriseerde aanpassing, zijn wij in staat de oorsprong hiervan te achterhalen door middel van uitgebreide logs.</p>		X	
<p>Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens?</p> <ul style="list-style-type: none"> - Laag = alleen in de toepassing - Midden = in de toepassing, maar ook in het proces (bijvoorbeeld leerresultaten) - Hoog = groot effect door bijvoorbeeld automatische beslissingen, veel koppelingen en veel transacties 	<p>Geplaatste gegevens zijn niet afhankelijk of hebben geen invloed op verdere processen. Een foutieve verandering heeft hierdoor geen invloed op een verdere verwerking.</p>	X		
<p>Leiden fouten of ongeautoriseerde veranderingen tot imagooverlies?</p> <ul style="list-style-type: none"> - Laag = nee - Midden = kortstondig imagooverlies - Hoog = langdurig imagooverlies 	<p>In het geval van een foutief of ongeautoriseerd bericht naar de ouders toe kan dit kortstondig leiden tot een imagooverlies.</p>		X	
<p>Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens?</p> <ul style="list-style-type: none"> - Laag = nee - Midden = ja, deze eisen stelselmatige controle (denk aan examenresultaten) - Hoog = ja, deze eisen stelselmatige controle en bewijs van werking (denk aan gegevens ten behoeve van bekostiging) 		X		
<p>Past de toepassing profilering** toe?</p> <ul style="list-style-type: none"> - Laag = nee - Midden = ja, maar deze leidt niet tot automatische beslissingen (alleen handmatig) - Hoog = ja, en deze leidt tot automatische beslissingen (door de toepassing zelf) 		X		

	Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = fouten veroorzaken ernstige of langdurige negatieve gevolgen	Alle gegevens, waaronder bijvoorbeeld profiel- en berichtgegevens, zijn direct door de eigenaar aan te passen. In het geval er foutieve gegevens zijn ingevoegd, zijn deze hooguit te zien tot deze weer zijn aangepast. Eventueel kan een medewerker van de helpdesk hierin ondersteuning bieden.	X
	I=	2	
	Omschrijving	Kenmerken	
Niveau 1: Laag	Integriteit is onbelangrijk. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	Bedrijfsproces tolereert enkele fouten Gegevens zijn volledig RPO* 7 dagen	
Niveau 2: Midden	Integriteit is beschermd. Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.	Een zeer beperkt aantal fouten is toegestaan Gegevens zijn volledig en juist RPO* 1 dag	
Niveau 3: Hoog	Integriteit is noodzakelijk. Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.	Bedrijfsproces eist foutloze informatie Gegevens zijn volledig, juist en actueel RPO* 4 uur	

* RTO is een kenmerk onder beschikbaarheid

** Profileren binnen de onderwijscontext is het maken van geautomatiseerde beslissingen die een leerling in aanmerkelijke mate treft (bijvoorbeeld adaptief leermateriaal wat invloed heeft op het niveau van de lesstof die een leerling wordt aangeboden). De AVG vraagt in dat geval om passende maatregelen om de betrokkene te beschermen.

Vertrouwelijkheid

Uitleg

Bedenk welke **gegevens** (bijvoorbeeld leerresultaten of leermateriaal) de ict-toepassing ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom. Controleer vervolgens aan de hand van de toelichting of het niveau passend is.

Vragen	Motivatie	Laag	Mid-den	Hoog
Welke type persoonsgegevens bevat de ict-toepassing? - Laag = geen - Midden = 'gewone' persoonsgegevens zoals NAW - Hoog = bijzondere persoonsgegevens (geloof, medisch, et cetera)	Alleen gewone persoonsgegevens zoals naam, e-mailadres en een optionele profielfoto worden opgeslagen. Daarnaast kan de volger, indien dit van toepassing is, optioneel een naam van het kind opgeven.		x	
Leiden datalekken tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies	Omdat het platform persoonsgegevens van de betreffende volgers voor de school/groep opslaat kan het bij een dataleg mogelijk tot een imagoverlies leiden.		x	
Zijn er contractuele of wettelijke verplichtingen voor de vertrouwelijkheid? - Laag = nee - Midden = ja, deze eisen bescherming - Hoog = ja, deze eisen bescherming, bewijs van werking en melding van inbreuk	Wettelijke eisen mbt de vertrouwelijkheid van leerlinggegevens.		x	
Kunnen er personen in gevaar worden gebracht als gevolg van het uitlekken van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = personen kunnen het slachtoffer worden van identiteitsfraude	Er worden geen adresgegevens of andere persoonlijke gegevens verwerkt welke bijvoorbeeld kunnen leiden tot een identiteitsfraude.	x		
Past de toepassing profilering* toe? - Laag = nee - Midden = ja, maar het profiel wordt niet opgeslagen/kan niet opgevraagd worden - Hoog = ja, en het profiel wordt opgeslagen/is inzichtelijk		x		
V= 2				
Niveau 1:	Omschrijving	Kenmerken		
Laag	Informatie is voor intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	Gegevens zijn alleen in te zien en te bewerken door personen binnen de organisatie.		

<p>Niveau 2:</p> <p>Midden</p>	<p>Informatie is vertrouwelijk.</p> <p>De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.</p>	<p>Gegevens alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.</p>	
<p>Niveau 3:</p> <p>Hoog</p>	<p>Informatie is geheim.</p> <p>De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.</p>	<p>Toegang is beperkt tot expliciet aangewezen personen binnen de organisatie. Beheerders hebben, waar mogelijk, geen toegang tot de gegevens. Beheerders maken alleen gebruik van persoonlijk herleidbare accounts.</p>	

*Profilering binnen de onderwijscontext is het maken van geautomatiseerde beslissingen die een leerling in aanmerkelijke mate treft (bijvoorbeeld adaptief leermateriaal wat invloed heeft op het niveau van de lesstof die een leerling wordt aangeboden). De AVG vraagt in dat geval om passende maatregelen om de betrokkene te beschermen.

BIJLAGE 4: Toelichting op maatregelen toetsingskader Certificeringsschema Informatiebeveiliging en Privacy ROSA

Deze bijlage is gebaseerd op het toetsingskader 1.2 binnen het certificeringsschema informatiebeveiliging en privacy ROSA:

https://www.edustandaard.nl/app/uploads/2018/02/4. Certificeringsschema_toetsingskader.xlsx

Categorie	Maatregelen	Voldaan / Niet voldaan	Uitleg
Beschikbaarheid			
	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Voldaan	
	Actuele dreigingen (DDoS, ransomware)	Voldaan	
Integriteit			
<i>gegevens</i>	Herleidbaarheid (gebruikers)	Voldaan	Wijzigingen worden bijgehouden en kunnen handmatig worden teruggedraaid n.a.v. deze logs.
<i>gegevens</i>	Backup	Voldaan	
<i>gegevens</i>	Application controls	Voldaan	Request logging d.m.v. Graylog
<i>gegevens</i>	Onweerlegbaarheid	Voldaan	
<i>toepassing</i>	Herleidbaarheid (technisch beheer)	Voldaan	
<i>toepassing</i>	Controle integriteit	Voldaan	
<i>toepassing</i>	Onweerlegbaarheid	Voldaan	
	Actuele dreigingen (DDoS, ransomware)	Voldaan	
Vertrouwelijkheid			
	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Voldaan	
	Toetsing	Voldaan	
	Actuele dreigingen (DDoS, ransomware)	Voldaan	