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 <Naam> B.V., gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Verwerker**"

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

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij <**concrete omschrijving van de door Verwerker in opdracht van Onderwijsinstelling te leveren producten/diensten**>, ('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 toegetreden Onderwijsinstelling of Leverancier;
e. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
g. Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
h. Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst. Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);
i. 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 verwerkingsactiviteiten[1] 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 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.

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

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 betrekt 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 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 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 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, 6, 9 en 12.

Bijlagen

Bijlage 1: Privacybijsluiter (beschikbaar per productgroep)
Bijlage 2: Beveiligingsbijlage (beschikbaar per productgroep)

Bijlage 1
Privacybijsluiter
Productgroep JimmyControl

Deze bijsluiter is een bijlage bij Verwerkersovereenkomst Odin Onderwijs B.V. h.o.d.n. Heutink ICT.

Deze bijsluiter is gebaseerd op de branchespecifieke privacybijsluiter van de Vereniging Digitale Onderwijs Dienstverleners (VDOD). De VDOD-bijsluiter is op zijn beurt gebaseerd op de privacybijsluiter bij de modelverwerkersovereenkomst behorende bij het Convenant. Dit model is afgestemd door de Initiatiefnemers van het Convenant en is gepubliceerd op de website van Edu-k. [https://www.edu-k.nl/]

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 bijsluiter 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 Privacybijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. De inhoud is evenzeer relevant voor klanten buiten de onderwijssector.

A) Algemene informatie

Naam product

Deze Privacybijsluiter betreft de productgroep JimmyControl. JimmyControl is een pakket waarin functionaliteiten op het gebied van MDM (mobile device management) en Classroom-management in combinatie worden ontsloten en aangeboden. MDM bestaat uit softwaretools die het beheer voeren over gekoppelde apparaten (hardware zoals laptops, tablets, etc) alsmede het beheer over de op deze gekoppelde apparaten gebruikte functionaliteiten (randapparatuur, software, apps, etc). Classroom-management voegt daar de functionaliteit aan toe om dit te beheren op het niveau van individuele en groepen leerlingen (met inbegrip van sturen, meekijken en controleren). Daarmee kan binnen JimmyControl onderscheid gemaakt worden in:

- Gebruikersbeheer
- Apparaatbeheer (al dan niet per leerling)
- Functionaliteitenbeheer (al dan niet per leerling)

In dit document wordt de hele productgroep JimmyControl, inclusief gerelateerde diensten, afgekort als “JimmyControl” (tenzij anders vermeld).

Naam Verwerker en vestigingsgegevens

Leverancier en Verwerker in relatie tot JimmyControl is:

- Odin Onderwijs B.V., Expolaan 50, 7556 BE Hengelo (Ov), Nederland
- Odin Onderwijs handelt onder de naam Heutink ICT

Nadere contactgegevens zie paragraaf H.

Terminologie-synoniemenlijst

De praktijk, de AVG, het Convenant en de Verwerkersovereenkomst en ook de onderwijssector (de belangrijkste markt waarbinnen Heutink ICT opereert) hanteren elk een eigen terminologie om partijen in de keten aan te duiden. Om dit document leesbaar te houden is er voor gekozen om daar waar mogelijk aan te sluiten bij de terminologie uit de algemene praktijk. Hieronder een synoniemenlijst (vertaaltabel) inzake de gehanteerde terminologie.

Begrip in dit document (algemene praktijk)	Begrip in AVG, Convenant en Verwerkersovereenkomst	Begrip in de onderwijssector (hoofdmarkt Heutink ICT)
Klant, de klantorganisatie	Verwerkingsverantwoordelijke	School, onderwijsinstelling, het onderwijs
Leverancier, Heutink ICT, Odin Onderwijs B.V.	Verwerker	Leverancier
Gebruiker	-	Leerling, leerkracht, medewerker, ouder/verzorger, onderwijs-deelnemer

Beknopte uitleg en werking product

De verwerking van persoonsgegevens binnen JimmyControl heeft (al dan niet optioneel) betrekking op:

- Het binnen de klantorganisatie centraal aanmaken en beheren van gebruikers in de rollen leerkracht of ICT-coördinator binnen de JimmyControl-omgeving, opdat zij gebruik kunnen maken van de functionaliteiten van JimmyControl;

- Het binnen de klantorganisatie centraal aanmaken en beheren van gebruikers (in de rollen leerling, leerkracht of ICT-coördinator) binnen de JimmyControl-omgeving, opdat deze leerlingen, leerkrachten en ICT-coördinatoren door middel van een unieke gebruikersnaam kunnen inloggen op de gekoppelde apparaten, nadat ze daartoe als gebruikers door JimmyControl zijn aangemerkt bij het ontsloten toepasselijke onderliggende MDM-pakket (in de praktijk vaak Microsoft Intune en/of Google Chrome Management Console);
- Het verkrijgen van toegang tot JimmyControl door middel van een inlogprocedure, alsmede het tonen van de naam van de ingelogde gebruiker in de userinterface van JimmyControl;
- Het identificeren van de gebruikers van gekoppelde apparaten, op het moment dat leerkrachten en/of ICT-coördinatoren de gekoppelde apparaten actief beheren. Op dat moment ziet de leerkracht of ICT-coördinator de naam en avatarfoto van de leerling.

Doelgroepen

Het product JimmyControl is bovenal gericht op gebruik binnen de doelgroepen primair onderwijs, VSO-instellingen, kinderopvang en voortgezet onderwijs.

Gebruikers

Het product JimmyControl is bovenal gericht op gebruik door, leerkrachten, intern begeleiders, stagiairs, remedial teachers, ICT-coördinatoren en schooldirecteuren. Leerlingen zijn zelf geen gebruikers van JimmyControl.

B) Basis- en optionele verwerkingen

Odin Onderwijs B.V. maakt een onderscheid tussen verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product enerzijds en optionele verwerkingen anderzijds. De exacte status van de door klant (en indien de klant een Onderwijsinstelling is, tevens de daar onder vallende scholen) afgenomen productonderdelen is zichtbaar via de Product- en Dienstenovereenkomst. Indien Heutink ICT bij aanvang van het gebruik een productonderdeel beschikbaar stelt aan de klant, is er pas sprake van een Verwerking, indien de klant tot daadwerkelijk feitelijk gebruik van het betreffende onderdeel overgaat.

Wanneer er binnen JimmyControl gebruik wordt gemaakt van zogenaamde ‘open velden’ (in de praktijk ook wel aangeduid als bijvoorbeeld ‘vrije tekstvelden’ of ‘vrije invoervelden’) alsmede de aanmaak en opslag van documenten, kan Heutink ICT geen invloed uitoefenen op de daarin verwerkte gegevens. Indien de klant in deze open velden en/of aangemaakte documenten Persoonsgegevens opneemt die niet zijn vermeld in deze Privacybijsluiter en/of langs die weg Persoonsgegevens gebruikt voor doeleinden die niet zijn vermeld in deze Privacybijsluiter, doet klant dit onder eigen verantwoordelijkheid.

Analoog aan bovenstaande alinea inzake ‘open velden’, beschouwt Heutink ICT ook het via de meekijkfunctie door leerkrachten en/of ICT-coördinatoren mogelijkerwijs verkregen zicht op eventuele op het leerlingscherm getoonde Persoonsgegevens niet als een verwerking onder de verantwoordelijkheid van Heutink ICT. Heutink ICT kan immers geen invloed uitoefenen op de door leerlingen op hun beeldschermen opgeroepen gegevens. Indien binnen de klantorganisatie Persoonsgegevens worden opgeroepen die niet zijn vermeld in deze Privacybijsluiter en/of langs die weg Persoonsgegevens gebruikt voor doeleinden die niet zijn vermeld in deze Privacybijsluiter, doet klant dit onder eigen verantwoordelijkheid.

C) Doeleinden voor het Verwerken van Persoonsgegevens

Het Convenant maakt inzake producten en dienst onderscheid in ‘Leermiddelen en Toetsen’ enerzijds en ‘School- en Leerlinginformatiemiddelen’ anderzijds (definities zie artikel 1 van het Convenant).

Heutink ICT levert met het product JimmyControl een product in de categorie:

~~I. Leermiddelen en Toetsen~~

II. School- en Leerlinginformatiemiddelen

Bovenstaande typering vertaalt zich in de toepasselijkheid van onderstaande tabel uit de VDOD-modelovereenkomst, inzake doelstellingen van gegevensverwerking in het kader van het product. Op de plaats van de begrippen ‘onderwijsinstelling’ en ‘onderwijsdeelnemers’ kan in deze tabel in breder verband ook ‘klant’ en ‘gebruikers’ gelezen worden.

Van toepassing:	Doeleinde (conform artikel 5 lid 2 Privacyconvenant):	
Zie details hier direct onder	**A**	De organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:
Nee		- De indeling en aanpassing van roosters;
Nee		- De analyse en interpretatie van leerresultaten;
Nee		- Het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
Ja		- Het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;
Nee		- De communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;
Nee		- Financieel beheer;
Nee		- 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;
Nee		- Het behandelen van geschillen;
Nee		- Het uitwisselen van Persoonsgegevens met Derden, waaronder:
Nee		o Toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
Nee		o Samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;
Nee		o Partijen betrokken bij de invulling van stage of leer-/ werkplekken voor zover noodzakelijk en wettelijk toegestaan;
Nee		o Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.
Ja	**B**	Het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
Ja	**C**	Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
Ja	**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;
Ja	**E**	De continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
Nee	**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;

Nee	**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;
Nee	**H**	Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;
Nee	**I**	De uitvoering of toepassing van een andere wet.

D) Categorieën en soorten Persoonsgegevens

1. Categorieën

Heutink ICT verwerkt met JimmyControl (optioneel) onderstaande categorieën Persoonsgegevens inzake Betrokkenen. Op de plaats van de begrippen ‘onderwijs’ en ‘onderwijsdeelnemers’ kan in deze tabel in breder verband ook ‘klantorganisatie’ en ‘gebruikers’ gelezen worden.

Van toepassing:	Categorie Persoonsgegevens:	Toelichting:
Zie detail hier direct onder	1. Contactgegevens	Naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, geslacht en soortgelijke voor communicatie benodigde gegevens.
Ja		Nota bene 1: Verwerker heeft alleen toegang tot de volgende gegevens: • Voornaam • Achternaam • Rol (alleen personeel) • Emailadres • Wachtwoord (versleuteld en, onomkeerbaar opgeslagen) • Klas (hoofdgroep) • IP-adres Nota bene 2: De hier genoemde gegevens worden door de ICT-coördinator aangemaakt (of op diens initiatief uitgelezen uit externe systemen). Dit betekent dat ervoor gekozen kan worden geanonimiseerde namen en email-adressen te hanteren. Doorgaans echter zal het gaan om herkenbare namen en emailadressen, waarmee het Persoonsgegevens worden in de zin van de AVG. Nota bene 3: De klantorganisatie maakt door het aanmaken (of uitlezen uit externe systemen) van emailadressen en wachtwoorden feitelijk eigen ID’s aan.
Nee	2. Onderwijs-deelnemernummer	Een administratienummer dat onderwijsdeelnemers identificeert
Nee	3. Nationaliteit en geboorteplaats	
Nee	4. Ouders, voogd	Gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers.
Nee	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;
Nee	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.

Nee	7. Studievoortgang	Gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: • Klas/leerjaar/ILT-code • Examinering • Studievoortgang en/of Studietraject • Begeleiding onderwijsdeelnemers, inclusief handelingplan • Aanwezigheidsregistratie
Ja	8. Onderwijsorganisatie	Gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen.
Nee	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.
Zie detail hier direct onder	10. Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut.
Ja		Gebruikers worden visueel gerepresenteerd door een avatar. Dit is een door de ICT-coördinator voor elke gebruiker te selecteren afbeelding, waarbij in de praktijk vaak gekozen wordt voor een pasfoto (waarmee het Persoonsgegevens zijn in de zin van de AVG).
Ja	11. Docent, zorgcoördinator, intern begeleider, decaan, mentor	Gegevens van docenten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen.
Nee	12. Overige gegevens, te weten [omschrijving opnemen]	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.
Nee	13. BSN/PGN	
Nee	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.

2. Soort Persoonsgegevens

Bovenstaande categorieën 3, 5 en 6 zijn bijzondere Persoonsgegevens in de zin van de AVG. Op grond van de aangegeven toepasselijkheid, kan geconcludeerd worden dat Verwerker:

- ~~Bijzondere Persoonsgegevens Verwerkt;~~
- Geen bijzondere Persoonsgegevens Verwerkt;

Bovenstaande categorieën 7, 9 en 13 worden (in ieder geval) gezien als gevoelige Persoonsgegevens in de zin van de AVG. Op grond van de aangegeven toepasselijkheid, kan geconcludeerd worden dat verwerker:

- ~~Gevoelige Persoonsgegevens Verwerkt;~~
- Geen gevoelige Persoonsgegevens Verwerkt;

3. Bewaartermijnen

Gezien de aard van het product JimmyControl worden de Persoonsgegevens die worden vastgelegd binnen JimmyControl slechts verwijderd op initiatief van de klant zelf. Deze verwijdering van gegevens kan daarbij plaatsvinden:

- Handmatig door gebruikers van de klant;
- Door Heutink ICT indien daartoe expliciet opdracht geven is door de klant.
- Door wederverkopers van Heutink ICT, daar waar deze wederverkopers inzake JimmyControl tevens optreden als formele beheerder (in plaats van Heutink ICT).

De klant is er derhalve zelf verantwoordelijk voor dat de Persoonsgegevens gedurende de juiste termijn worden bewaard en vernietigd. Door de klant vernietigde gegevens blijven in JimmyControl op de achtergrond gedurende maximaal 90 dagen opgeslagen, waarna ze vervolgens ook door Heutink ICT onomkeerbaar vernietigd worden.

E) Uitwerking Verwerkingen Persoonsgegevens en doeleinden per afgenomen dienst

Onderstaande tabel specificeert welke Persoonsgegevens (zie paragraaf D, nummers 1 t/m 14) binnen welk (al dan niet optionele) product(onderdeel) worden Verwerkt op grond van welk doeleinde (zie paragraaf C, letters A t/m I). Voor alle genoemde categorieën Persoonsgegevens geldt dat deze tevens worden Verwerkt ten behoeve van doeleinde E (back-ups, onderhoud en ondersteuning).

Persoonsgegevens 1 t/m 14 (zie paragraaf D):	Product(onderdeel) inclusief subverwerkers (zie tevens paragraaf G):	Doeleinde gebruik A t/m I (zie paragraaf C):
1 Contactgegevens	JimmyControl gebruikersbeheer JimmyControl apparaatbeheer JimmyControl functionaliteitbeheer	B, C, D A, B, C, D A, B, C, D
8 Onderwijsorganisatie	JimmyControl gebruikersbeheer JimmyControl apparaatbeheer JimmyControl functionaliteitbeheer	B, C, D B, C, D B, C, D
10 Beeldmateriaal	JimmyControl gebruikersbeheer JimmyControl apparaatbeheer JimmyControl functionaliteitbeheer	N.v.t. A A
11 Docent, zorgcoördinator, intern begeleider, Decaan, mentor	JimmyControl gebruikersbeheer JimmyControl apparaatbeheer JimmyControl functionaliteitenbeheer	B, C, D B, C, D B, C, D

F) Opslag Verwerking Persoonsgegevens:

De opslag en Verwerking van Persoonsgegevens binnen het product JimmyControl vindt plaats op de locatie van Microsoft Azure Europa-west te Nederland. Vanaf 01-01-2020 zal dit vermoedelijk zijn gewijzigd naar Subverwerker Previder (zie paragraaf G).

G) Subverwerkers

Toestemming inschakelen Subverwerkers

Klant geeft Heutink ICT een algemene toestemming voor het inschakelen van een Subverwerker. Heutink ICT heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan klant, en klant daartegen bezwaar kan maken binnen een redelijke periode. De klant zal de door haar verleende toestemming niet op onredelijke gronden weigeren.

Heutink ICT zal met de Subverwerkers die worden ingezet voor de verwerking van de Persoons-gegevens een verwerkersovereenkomst sluiten waarin minimaal dezelfde verplichtingen staan als waaraan zij zelf gebonden is op grond van de Verwerkersovereenkomst.

Gehanteerde Subverwerkers

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

Naam	Vestigingsplaats	Land van opslag en Verwerking	Omschrijving taak/dienst	Standaard of optioneel product-onderdeel
Microsoft	Datacenter, Nederland	Nederland	Hosting provider (huidig)	Standaard
Previder B.V.	Hengelo (Ov.), Nederland	Nederland	Hosting provider (beoogd vanaf 01-01-2020)	Standaard

Aanvullende details inzake belangrijkste Subverwerkers

Microsoft biedt onder de naam Azure wereldwijd hosting aan. Daarbij maakt Microsoft gebruik van vele datacenters, die vallen onder de wetgeving van het land van vestiging. Voor JimmyControl maakt Heutink ICT gebruik van het Europa-west datacenter, gesitueerd in Nederland. De dataverwerking valt daarmee onder de Nederlandse en Europese wetgeving.

Previder B.V. maakt net als Heutink ICT onderdeel uit van de Odin Groep B.V. Previder is de hosting provider van Heutink ICT. Previder is in het bezit van onder andere de volgende certificeringen: ISO 27001, ISO 9001, SOC 2 Type 2. De Persoonsgegevens die Heutink ICT in opdracht van klanten verwerkt worden door Previder op de volgende locaties verwerkt:

- Previder Datacenter 1 (PDC 1), Expolaan 50, 7556 BE Hengelo (Ov), Nederland
- Previder Datacenter 2 (PDC 2), Barnsteenstraat 15, 7554 TC Hengelo (Ov), Nederland)

Criterium Subverwerker

Indien Heutink ICT de verwerking van Persoonsgegevens uit eigener beweging onderbrengt bij een derde, interpreteert Heutink ICT deze derde als zijnde een Subverwerker.

Daar waar Heutink ICT softwaretools van derden incorporeert in JimmyControl, waarbij dit softwaretool echter geen off premise-connectie kent met de leverancier van het softwaretool, interpreteert Heutink ICT deze derde niet als zijnde een Subverwerker. De gehele werking van het softwaretool wordt in dat geval beschouwd als de verantwoordelijkheid van Heutink ICT als Verwerker.

Daar waar Heutink ICT de gebruiker expliciet vraagt om akkoord te gaan met het delen van op attribuutniveau gespecificeerde gegevens met derden, interpreteert Heutink ICT deze derde niet als zijnde een Subverwerker. In dat geval zal de klant zelf het aangaan van een Verwerkersovereenkomst met deze derde moeten overwegen.

Productivity suites

Productivity suites zijn softwareomgevingen gericht op werkzaamheden zoals onder andere tekstverwerken, presentaties maken, rekenwerk verrichten, communicatie, samenwerken en (cloud)opslag van bestanden. Bekende productivity suites zijn Microsoft Office365 (Word, PowerPoint, Excel, Outlook, Teams, SharePoint, OneDrive, etc) en Google G-Suite (Documenten, Presentaties, Spreadsheets, Gmail, Hangouts, Drive, etc).

Heutink ICT is betrokken bij de productivity suites van haar klanten, door de omgeving op te leveren en te beheren met de gewenste functionele instellingen en de gewenste gekoppelde gebruikers (identificatie op gebruikersnaam, voornaam, achternaam, leerjaar, groep(en) en rol(len)). Heutink ICT is evenwel niet betrokken bij de gegevensverwerking en gegevensopslag binnen de suites, aangezien dit rechtstreeks plaatsvindt tussen de klant en de suite-provider (zoals Microsoft en Google).

Heutink ICT stelt zich dan ook op het standpunt dat ze ten aanzien van het (faciliteren van het) werken met productivity suites geen Verwerker is in het kader van de Algemene Verordening Gegevens-bescherming (AVG), zulks althans niet verderstrekkend dan het correcte beheer en met toestemming van de klant doorkoppelen van identificatiegegevens. Dit betekent dat de aanbieders van productivity suites geen subverwerker zijn.

MDM-pakketten

MDM-pakketten (mobile device management-pakketten) zijn softwaretools die het beheer voeren over gekoppelde apparaten (hardware zoals laptops, tablets, etc) alsmede het beheer over de op deze gekoppelde apparaten gebruikte functionaliteiten (randapparatuur, software, apps, etc). In een schoolomgeving stellen ze bijvoorbeeld de leerkracht en/of ICT-coördinatorbeheerder in staat om de door de leerlingen gebruikte laptops te beheren, in de zin dat de leerkracht desgewenst overal (of selectief) dwingend dezelfde software opstart of overal (of selectief) dwingend de luidsprekers uit zet.

Heutink ICT is betrokken bij de MDM-pakketten van haar klanten, door het MDM in te richten en te beheren met de gewenste instellingen, de gewenste gekoppelde apparaten en de gewenste gekoppelde gebruikers (identificatie op gebruikersnaam). Heutink ICT is evenwel niet betrokken bij de gegevensverwerking en gegevensopslag binnen de mogelijkheden van de apparaten, aangezien dit rechtstreeks plaatsvindt op het apparaat en daarmee tussen de klant en de gebruikers enerzijds en de partij achter de aangeroepen functionaliteit anderzijds (zoals webbrowsing via Chrome of een app opstarten zoals Youtube).

Heutink ICT stelt zich dan ook op het standpunt dat ze ten aanzien van het (faciliteren van het) werken met MDM-pakketten geen Verwerker is in het kader van de Algemene Verordening Gegevens-bescherming (AVG), zulks althans niet verderstrekkend dan het correcte beheer en met toestemming van de klant doorkoppelen van identificatiegegevens. Dit betekent dat de aanbieders van MDM-pakketten geen subverwerker zijn.

H) Contactgegevens

Voor vragen of opmerkingen over deze Privacybijsluiter en/of over de werking van het product JimmyControl, kunt u contact opnemen langs onderstaande wegen.

Contactgegevens:

- Odin Onderwijs B.V., Expolaan 50, 7556 BE Hengelo (Ov), Nederland
- Odin Onderwijs handelt onder de naam Heutink ICT
- De JimmyControl-helpdesk is telefonisch bereikbaar via 074-2404666
- Voor alle overige vragen kunt u bellen naar 074-2404606 of mailen naar info@heutink-ict.nl

Links:

- www.heutink-ict.nl
- www.jimmycontrol.nl

Heutink ICT heeft een functionaris gegevensbescherming aangesteld die tevens de rol van Security Officer vervuld. Binnen Heutink ICT houdt hij toezicht op de toepassing en naleving van de AVG en de beveiliging in het algemeen. Voor vragen aan de Security Officer van Heutink ICT kunnen klanten telefonisch of per email contact opnemen via bovenstaande contactgegevens.

I) Versie

Deze Privacybijsluiter is voor het laatst bijgewerkt op per 24 september 2019.

Bijlage 2
Beveiligingsbijlage
Productgroep JimmyControl

Deze bijlage is een bijlage bij Verwerkersovereenkomst Odin Onderwijs B.V. h.o.d.n. Heutink ICT.

Deze bijlage is gebaseerd op de branchespecifieke bijlage van de Vereniging Digitale Onderwijs Dienstverleners (VDOD). Deze VDOD-bijlage is op zijn beurt gebaseerd op bijlage 2 bij de modelbewerkersovereenkomst behorende bij het Convenant. Dit model is afgestemd door de Initiatiefnemers van het Convenant en is gepubliceerd op de website van Edu-k. [https://www.edu-k.nl]

Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht 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 weergave van die maatregelen. In het kader van het organiseren en aantonen van deze voornoemde maatregelen, maakt Verwerker gebruik van (de meest recente versie van) het in het onderwijs ontwikkelde ‘Certificeringsschema informatiebeveiliging en privacy ROSA’. De inhoud is evenzeer relevant voor klanten buiten de onderwijssector.

Algemene informatie

Naam product

Deze Privacybijsluiter betreft de productgroep JimmyControl. JimmyControl is een pakket waarin functionaliteiten op het gebied van MDM (mobile device management) en Classroom-management in combinatie worden ontsloten en aangeboden. MDM bestaat uit softwaretools die het beheer voeren over gekoppelde apparaten (hardware zoals laptops, tablets, etc) alsmede het beheer over de op deze gekoppelde apparaten gebruikte functionaliteiten (randapparatuur, software, apps, etc). Classroom-management voegt daar de functionaliteit aan toe om dit te beheren op het niveau van individuele en groepen leerlingen (met inbegrip van sturen, meekijken en controleren). Daarmee kan binnen JimmyControl onderscheid gemaakt worden in:

- Gebruikersbeheer
- Apparaatbeheer (al dan niet per leerling)
- Functionaliteitenbeheer (al dan niet per leerling)

In dit document wordt de hele productgroep JimmyControl, inclusief gerelateerde diensten, afgekort als “JimmyControl” (tenzij anders vermeld).

Terminologie-synoniemenlijst

De praktijk, de AVG, het Convenant en de Verwerkersovereenkomst en ook de onderwijssector (de belangrijkste markt waarbinnen Heutink ICT opereert) hanteren elk een eigen terminologie om partijen in de keten aan te duiden. Om dit document leesbaar te houden is er voor gekozen om daar waar mogelijk aan te sluiten bij de terminologie uit de algemene praktijk. Hieronder een synoniemenlijst (vertaaltabel) inzake de gehanteerde terminologie.

Begrip in dit document (algemene praktijk)	Begrip in AVG, Convenant en Verwerkersovereenkomst	Begrip in de onderwijssector (hoofdmarkt Heutink ICT)
Klant, de klantorganisatie	Verwerkingsverantwoordelijke	School, onderwijsinstelling, het onderwijs
Leverancier, Heutink ICT, Odin Onderwijs B.V.	Verwerker	Leverancier
Gebruiker	-	Leerling, leerkracht, medewerker, ouder/verzorger, onderwijsdeelnemer

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

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

Heutink ICT hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke Persoonsgegevens. Medewerkers van Heutink ICT hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie. Hieronder wordt uitgewerkt welke (groepen) medewerkers van Heutink ICT toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

Groepen van medewerkers en Persoonsgegevens:	Handelingen:
Medewerkers van de afdeling Service &Support (helpdesk) hebben toegang tot de binnen JimmyControl aanwezige persoonsgegevens (categorieën 1, 8, 10 en 11, hoofdstuk D, zie corresponderende Privacybijsluiter).	De handelingen van de betreffende medewerkers zijn gericht op de ondersteuning van eindgebruikers, meer in het bijzonder het beantwoorden van gebruikers-vragen en het oplossen van eventuele storingen.
Medewerkers van de afdeling Projectbureau hebben toegang tot de binnen JimmyControl aanwezige persoonsgegevens (categorieën 1, 8, 10 en 11, hoofdstuk D, zie corresponderende Privacybijsluiter).	De handelingen van de betreffende medewerkers zijn gericht op het inrichten van nieuwe klantomgevingen.
Medewerkers van de afdeling Innovatie & Ontwikkeling (daaronder begrepen de subafdeling Beheer) hebben toegang tot de databases, met in begrip van databases met Persoonsgegevens. De toegang wordt gelogd.	De handelingen van de betreffende medewerkers zijn gericht op de ontwikkeling, optimalisatie, goede werking en performance van de ICT-systemen.
Andere dan hierboven genoemde medewerkers hebben geen inzage in of toegang tot Persoonsgegevens.	N.v.t.
Daar waar wederverkopers van Heutink ICT inzake JimmyControl optreden als formele beheerder (in plaats van Heutink ICT), hebben corresponderende medewerkers toegang tot de corresponderende informatie.	Corresponderende handelingen.

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

Heutink ICT heeft het Certificeringsschema van Edu-K gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor JimmyControl. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Toetsvorm:	Self-assessment
Uitvoerder toets:	Odin Onderwijs B.V. h.o.d.n. Heutink ICT, Security Officer
BIV-classificatie:	Beschikbaarheid =1, Integriteit = 2, Vertrouwelijkheid = 1

Categorie	**Maatregelen**	**Compliance** Voldaan/ niet voldaan/ alternatieve maatregel	**Uitleg** Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven.
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Voldaan	
	Actuele dreigingen	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	
	Backup	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Actuele dreigingen	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	Voldaan	

Organisatie van informatiebeveiliging en communicatieprocessen:

- Heutink ICT heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid;
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid;
- Heutink ICT heeft een proces ingericht voor communicatie over informatiebeveiligings-incidenten.

Medewerkers:

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatie-beveiligingsafspraken gemaakt;
- Heutink ICT stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging;
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Fysieke beveiliging en continuïteit van de middelen:

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf;
- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren;
- Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienst-verlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving;
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's. Netwerk-, server- en applicatiebeveiliging en onderhoud;
- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen;
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord;
- De digitale leermiddelen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. Wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen;
- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd op basis van patchmanagement;
- Gegevens die binnen applicaties worden verwerkt zijn geclassificeerd op risico's;
- Penetratietests en vulnerability assessments worden periodiek uitgevoerd;
- Niet (meer) gebruikte informatie wordt verwijderd;
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan;
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van klanten vindt waar mogelijk versleuteld plaats.

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

Interne evaluatie en externe controle

Naast periodieke interne evaluatie, worden de getroffen beveiligingsmaatregelen en aanwezige systemen van Heutink ICT jaarlijks gecontroleerd aan de hand van (inter)nationaal erkende normen en standaarden voor informatiebeveiliging door een extern bedrijf dat is gespecialiseerd in

cybersecurity. Daarnaast voorziet het beveiligingsbeleid van Heutink ICT in interne processen om kwetsbaarheden te identificeren.

Audit en certificering

De Verwerkersovereenkomst biedt klanten de mogelijkheid om in overleg met Heutink ICT de naleving van de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens te controleren door middel van een audit. Daarnaast kan Heutink ICT de naleving van haar verplichtingen ook aantonen door middel van een geldige (inter)nationaal erkende certificering.

Heutink ICT is in het bezit van diverse certificeringen waaronder ISO 9001, ISO 27001 en een SOC 2 type 2 certificering. Op verzoek van een klant zal Heutink ICT de betreffende certificaten kosteloos verstrekken. Op deze manier wil Heutink ICT in beginsel voldoen aan haar contractuele verplichting om de klant in staat te stellen om toezicht te houden op de verwerking van de persoonsgegevens.

Indien een klant ondanks het overleggen van de diverse certificeringen de wens heeft om een audit uit te voeren naar de naleving van de verwerkersovereenkomst en toepasselijke wet- en regelgeving, treedt Heutink ICT graag in overleg om samen daarbij het middel en het doel in balans te houden.

Rapportage en contact

Het verbeteren van de beveiliging is een constant proces. Daarom kan Heutink ICT wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen als zij van mening is dat de betreffende wijziging noodzakelijk is om passende technische en organisatorische maatregelen te blijven bieden en om haar certificeringen te behouden. Heutink ICT zal de door haar genomen beveiligingsmaatregelen nooit naar een lager niveau bijstellen.

Heutink ICT zal alle wijzigingen vastleggen. Klanten worden alleen van significante wijzigingen op de hoogte gesteld. Alle wijzigingen worden jaarlijks gecommuniceerd door middel van aanpassing van deze Beveiligingsbijlage bij de Verwerkersovereenkomst. Deze aanpak voorkomt dat voor alle wijzigingen, hoe triviaal en klein ook, steeds toestemming nodig zijn van alle klanten.

Voor vragen of opmerkingen over deze Beveiligingsbijlage en/of over de (veilige) werking van het product JimmyControl, kunt u contact opnemen langs onderstaande wegen. Zeker indien u een beveiligingsrisico's vermoedt of constateert, verzoeken wij u om contact op te nemen.

Contactgegevens:

- Odin Onderwijs B.V., Expolaan 50, 7556 BE Hengelo (Ov), Nederland
- Odin Onderwijs handelt onder de naam Heutink ICT
- De JimmyControl-helpdesk is telefonisch bereikbaar via 074-2404666
- Voor alle overige vragen kunt u bellen naar 074-2404606 of mailen naar info@heutink-ict.nl

Links:

- www.heutink-ict.nl
- www.jimmycontrol.nl

Heutink ICT heeft een functionaris gegevensbescherming aangesteld die tevens de rol van Security Officer vervuld. Binnen Heutink ICT houdt hij toezicht op de toepassing en naleving van de AVG en de beveiliging in het algemeen. Ook voor vragen aan de Security Officer van Heutink ICT kunnen klanten telefonisch of per email contact opnemen via bovenstaande contactgegevens.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

Ondanks diverse in deze Beveiligingsbijlage beschreven maatregelen om de gegevensverwerking te beveiligen, kan er toch een inbreuk in verband met de Persoonsgegevens ontstaan. Onder een inbreuk in verband met Persoonsgegevens wordt op grond van artikel 4, aanhef, sub 12 AVG verstaan: 'Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'. Dergelijke inbreuken worden in het spraakgebruik 'datalekken' genoemd.

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Heutink ICT monitort 24/7 haar dienstverlening om eventuele ongeoorloofde of onrechtmatige toegang tot gegevens te identificeren. Signalen die duiden op een Datalek worden direct gemeld aan – en opgepakt door – de Security Officer van Verwerker, die analyseert en beoordeelt of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld

Heutink ICT heeft intern een procedure ingericht voor het afhandelen van datalekken. Wanneer zich een Datalek voordoet wordt de klant door Heutink ICT zonder onredelijke vertraging per email geïnformeerd (dat wil zeggen zo snel mogelijk en in beginsel zeker binnen 24 uur). Afhankelijk van de situatie behoudt Heutink ICT zich het recht voor om klanten via haar website, officiële sociale mediakanalen, officiële distributeurs en/of handelsagenten te informeren over het betreffende datalek. Voor vervolgacties of vragen kan telefonisch of per email contact worden opgenomen met de helpdesk via de contactgegevens zoals opgenomen elders in dit document.

De te delen informatie

Indien zich een Datalek voordoet zal Heutink ICT de volgende informatie delen met de betreffende klant:

- De kenmerken van het incident, zoals: de datum en het tijdstip van constatering, een samenvatting van het incident, de kenmerken en de aard van het incident (op wat voor onderdeel van de beveiliging ziet het datalek, 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 en/of verdere schade te voorkomen;
- De maatregelen die zijn getroffen om een dergelijk datalek in de toekomst te voorkomen;
- Het benoemen van de groep betrokkenen die gevolgen kunnen ondervinden van het datalek en de mate waarin zij deze gevolgen kunnen ondervinden;
- De omvang van de groep betrokkenen;
- Het soort persoonsgegevens dat door het incident is getroffen.

Melding bij de Autoriteit Persoonsgegevens

Heutink ICT zal alle datalekken melden aan de klant. Niet alle datalekken dienen door klant gemeld te worden bij de Autoriteit Persoonsgegevens. Op basis van de artikelen 33 en 34 AVG is de klant verplicht om inbreuken in verband met persoonsgegevens, die waarschijnlijk een risico voor de privacy inhouden, indien mogelijk binnen 72 uur te melden aan de Autoriteit Persoonsgegevens. Wanneer een inbreuk waarschijnlijk een hoog risico inhoudt voor de privacy dan moet de klant de inbreuk ook onverwijld meedelen aan de betrokkenen (bijvoorbeeld inzake leerlingen op een school, melding doen aan de ouders van de betreffende kinderen). De beoordeling of de inbreuk

waarschijnlijk een risico of waarschijnlijk een hoog risico voor de privacy inhoudt en dus gemeld moet worden bij de Autoriteit Persoonsgegevens en/of betrokkenen moet door de klant worden verricht. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 AVG moeten worden gemeld aan Autoriteit Persoonsgegevens en/of Betrokkene, blijft te allen tijde de verantwoordelijkheid van de klant.

De kosten voor het melden van het datalek bij de klant en het nemen van maatregelen om herhaling en verdere schade te voorkomen komen voor rekening van de klant, tenzij het betreffende datalek het gevolg is van een toerekenbare tekortkoming aan de zijde van Heutink ICT.

Indien een concrete situatie zich daartoe leent, dan kan Heutink ICT een (eerste) melding van een Datalek doen aan de Autoriteit Persoonsgegevens. De klant wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

Versie

Deze Beveiligingsbijlage is voor het laatst bijgewerkt per 24 september 2019.