Stimuliz Licensing B.V.

Kloosterweg 1

6412 CN Heerlen

Mail info@stimuliz.com

VERWERKERSOVEREENKOMST

ONDERGETEKENDEN:

Partijen:

1. Het bevoegd gezag van **{{Organisatie}}**, gevestigd en kantoorhoudende aan **{{Adres}}**, **{{Postcode}}** te **{{Plaats}}**, te dezen rechtsgeldig vertegenwoordigd door **{{Tekenbevoegde}}**, hierna te noemen: **"Onderwijsinstelling"**.

en

2. De besloten vennootschap met beperkte aansprakelijkheid **Stimuliz Licensing B.V.**, dochteronderneming van Stimuliz B.V., gevestigd en kantoorhoudende aan Kloosterweg 1, te 6412 CN Heerlen, te dezen rechtsgeldig vertegenwoordigd door Wim Schrooten, hierna te noemen: **"Verwerker"**,

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

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan van Stimuliz, een webbased leerlingvolgsysteem, ('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. Keten iD: een pseudoniem van een persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het Keten iD wordt ook ECK iD genoemd;

j. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;

k. Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;

l. Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;

m. Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;

n. Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;

o. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;

p. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;

q. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;

r. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem,

studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerlingvolgsysteem;

s. Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);

t. Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;

u. AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG);

v. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.

2. De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.

3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in Bijlage 1, die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Onderwijsinstelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.

2. Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.

3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker 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 die onder hun verantwoordelijkheid plaatsvinden.

5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.

6. Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4: Privacyconvenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechterlijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking van dat wettelijke voorschrift dan wel de rechterlijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.

2. Een overzicht van onder meer de categorieën Persoonsgegevens en het doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacybijsluiter bij deze Verwerkersovereenkomst.

3. De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de Verwerkersverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt

4. Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.

5. *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. *<u>SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS</u>:*

    a. *Convenantspartijen die Leermiddelen en Toetsen ontwikkelen en aanbieden (hierna te noemen: Leermiddelenleverancier), zullen jaarlijks ten behoeve van het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, (welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld) de Privacy Bijsluiter voor die Leermiddelen en Toetsen aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt (met betrekking tot de Leermiddelen en Toetsen die op de desbetreffende leermiddelenlijsten worden opgenomen).*

    b. *Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.*

    c. *De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.*

    d. *Onderwijsinstelling vrijwaart Verwerker (distributeur) voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Leermiddelenleverancier, en de Onderwijsinstelling vrijwaart de Leermiddelenleverancier voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Verwerker (distributeur).*

    e. *De verantwoordelijkheid van Verwerker (distributeur) voor het beheer van de Persoonsgegevens houdt op, op het moment dat de Leermiddelenleverancier die gegevens heeft ontvangen van Verwerker (distributeur).*

Artikel 6: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij 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 gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, tot verstrekking verplicht is.

3. Verwerker onthoudt zich van verstrekking of bekendmaking van Persoonsgegeven aan een Derde, tenzij deze verstrekking of bekendmaking plaatsvindt in opdracht van Onderwijsinstelling respectievelijk wanneer dit noodzakelijk is om te voldoen aan een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker - tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling

onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.

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

Artikel 7: Beveiliging en controle

1. Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

2. Naast de maatregelen als genoemd in artikel 32 lid 1 AVG, worden onder meer de volgende maatregelen - waar passend - genomen:

    a. een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;

    b. maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;

    c. het regelen van procedures rondom het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering, en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren.

3. Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.

4. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze van de verklaringen die Verwerker verstrekt over de afgesproken beveiligingsmaatregelen.

5. De Verwerker stelt in goed overleg de Onderwijsinstelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken.

6. In aanvulling op de voorgaande leden heeft Onderwijsinstelling te allen tijde het recht om, in overleg met de Verwerker en met inachtneming van een redelijke termijn, de naleving van Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, de Product- en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde externe deskundige:

    a. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.

    b. De auditor verstrekt het auditrapport alleen aan Partijen.

    c. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.

d. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.

e. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken

1. Partijen hebben een passend beleid voor de omgang met Datalekken.

2. Indien Onderwijsinstelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover *zonder onredelijke vertraging* informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt in geval van een Datalek alle relevante informatie aan Onderwijsinstelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.

3. Verwerker informeert Onderwijsinstelling *onverwijld* indien een vermoeden bestaat dat een Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34,lid 1, AVG.

4. Verwerker stelt bij een Datalek de Onderwijsinstelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Onderwijsinstelling daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens, en meer in het bijzonder (verdere) schending van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, te voorkomen of te beperken.

5. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. In geval een Datalek bij Verwerker meerdere Onderwijsinstellingen in gelijke mate treft, kan Verwerker, na overleg met een of meerdere Verwerkingsverantwoordelijken, namens de Onderwijsinstellingen een melding doen van het Datalek aan de Autoriteit Persoonsgegevens. Van het voornemen hiervan zal Verwerker Onderwijsinstelling onverwijld (en zo mogelijk voorafgaand aan de melding) in kennis stellen.

6. In geval van het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Onderwijsinstelling de Betrokkenen informeren over het Datalek.

7. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.

8. Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

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

Artikel 9 Bijstand

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

    a. het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;

    b. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;

    c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;

    d. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;

    e. het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.

2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.

3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

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

1. Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land of internationale organisatie indien Onderwijsinstelling daarvoor specifieke Schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Onderwijsinstelling voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de Europese Economische Ruimte of aan een internationale organisatie zoals bedoeld in artikel 4 lid 26 AVG, dan zien Partijen er op toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien gegevens worden doorgegeven aan een derde land of een internationale organisatie, dan wordt dit in Bijlage 1 bij deze Verwerkers-overeenkomst aangegeven, inclusief een opgave van de landen waar, of internationale organisaties door wie, de Persoonsgegevens worden verwerkt. Daarbij wordt tevens aangegeven op welke wijze is voldaan aan de voorwaarden op basis van de AVG voor doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

Artikel 11: Inschakeling Subverwerker

1. Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkers-overeenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in de Privacybijsluiter.

2. Tijdens de duur van de Verwerkersovereenkomst licht Verwerker Onderwijsinstelling in over een voorgenomen toevoeging van een nieuwe Subverwerker of wijziging in de samenstelling van de bestaande Subverwerkers, waarbij Onderwijsinstelling de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

3. Verwerker is verplicht iedere Subverwerker via een overeenkomst of andere rechtshandeling minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd. Hieronder vallen onder meer de verplichting om de Persoonsgegevens niet verder te Verwerken anders dan in het kader van deze Verwerkersovereenkomst is overeengekomen, en de verplichting tot het nakomen van de geheimhoudingsverplichtingen, meldingsverplichtingen, medewerkingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens zoals in deze Verwerkersovereenkomst vastgelegd. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Verwerkers-overeenkomsten, of van de relevante passages uit de Verwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 11, lid 1, van deze overeenkomst ingeschakelde Subverwerker.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.

2. Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.

3. Verwerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.

4. Verwerker zal alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkers-overeenkomst en zal waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Aansprakelijkheid

1. Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Product- of Dienstenovereenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:

    a. verhaalsactie op grond van artikel 82 AVG; of

    b. schadevergoedingsactie uit hoofde van deze Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthouder betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

    Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken partij op grond van de geldende wet- of regelgeving ter beschikking staat.

2. Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 14 lid 2.

3. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthouder, beiden in verband met deze Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de

andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 14: Tegenstrijdigheid en wijziging Verwerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.

2. Indien Partijen van de artikelen in de Model Verwerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Verwerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.

3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens en de doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in Bijlage 1 worden opgenomen.

4. Wijzigingen in de artikelen van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.

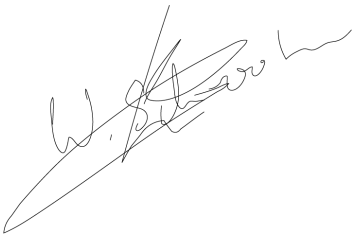
5. In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 15: Duur en beëindiging

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.

2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 5, lid 1, en de artikelen 6, 9 en 12.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,	Verwerker,
	
……(handtekening)	
Naam: ……..	Naam: Wim Schrooten
Functie:……..	Functie: Directeur
Datum: ……..	Datum: ……..

Bijlage 1: Privacybijsluiter

Bijlage 2: Beveiligingsbijlage

Bijlage 3: Classificatie Certificeringsschema Informatiebeveiliging en privacy ROSA

Bijlage 4: Toetsingskader Certificeringsschema Informatiebeveiliging

BIJLAGE 1: Privacybijsluiter

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 Privacy bijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. De Privacy bijsluiter is een bijlage bij de Modelverwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.

A. Algemene informatie

Naam product en/of dienst	Stimuliz
Naam Verwerker en vestigingsgegevens	Stimuliz Licensing B.V., dochteronderneming van Stimuliz B.V. te Heerlen
Link naar leverancier	https://stimuliz.com
Beknopte uitleg en werking	Monitoring en verbetering van gezondheidsaspecten, zoals biometrie, motoriek sport- en beweegbeleving en sociaal-emotionele ontwikkeling, van kinderen.
Doelgroep	Primair onderwijs, Voortgezet onderwijs
Gebruikers	Onderwijsinstellingen in het PO en VO

B. Omschrijving specifieke diensten

Bij de afname van Stimuliz kan de Onderwijsinstelling, naast de standaard / basismodule, kiezen voor verschillende optionele modules. In het onder E opgenomen schema wordt (in dat geval per module) weergegeven welke Persoonsgegevens er worden Verwerkt en voor welke (onder C opgenomen) doeleinden dit gebeurt.

Status afgenomen modules en activatie van optionele Verwerkingen door feitelijk gebruik

De exacte status van de door Onderwijsinstelling (en de onder de Onderwijsinstelling vallende scholen) afgenomen diensten/modules is zichtbaar via een beheerpagina. Indien Verwerker bij aanvang van het gebruik alle modules in zijn product en/of dienst beschikbaar stelt aan de Onderwijsinstelling, is er pas

sprake van een Verwerking, indien de Onderwijsinstelling tot daadwerkelijk gebruik van de betreffende module overgaat.

Wanneer binnen Stimuliz gebruik wordt gemaakt van zogenaamde ‘open velden’, kan Verwerker geen invloed uitoefenen op de daarin Verwerkte gegevens. Indien de Onderwijsinstelling in de open velden Persoonsgegevens opneemt die niet zijn worden vermeld in deze Privacy Bijsluiter en/of Persoonsgegevens gebruikt voor doeleinden die niet zijn vermeld in deze Privacy Bijsluiter, doet Onderwijsinstelling dit onder eigen verantwoordelijkheid.

C. Doeleinden voor het verwerken van gegevens

De volgende doelstellingen van gegevensverwerking zijn mogelijk van toepassing op onze diensten:

Van toepassing	**Categorie**	**Doeleinde (conform artikel 5 lid 1 Privacyconvenant)**
Ja, deels	A	de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder: ~~- de indeling en aanpassing van roosters;~~ - de analyse en interpretatie van leerresultaten; - het bijhouden van persoonlijke ~~(waaronder medische)~~ omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs; - het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling; - de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling; - financieel beheer; - 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; ~~- het behandelen van geschillen;~~ - het uitwisselen van Persoonsgegevens met Derden, waaronder: - toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak; - samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen; ~~- partijen betrokken bij de invulling van stage of leer-/werkplekken voor zover noodzakelijk en wettelijk~~

		~~toegestaan;~~ - Onderwijsinstellingen in geval 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;
Ja	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;
Ja	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.~~

In het onder E opgenomen schema wordt per module weergegeven welke (onder D opgenomen) Persoonsgegevens worden Verwerkt en voor welke (onder C opgenomen) doeleinden dit gebeurt.

D. Categorieën en soorten persoonsgegevens

Verwerkers geeft hieronder aan welke categorieën Persoonsgegevens er (al dan niet optioneel) kunnen worden verwerkt binnen Stimuliz. In het onder E opgenomen schema wordt per module weergegeven welke (onder D opgenomen) Persoonsgegevens worden verwerkt en voor welke (onder C opgenomen) doeleinden dit gebeurt.

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

Van toepassing	**Categorie**	**Toelichting**
Ja, deels	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;
Nee	~~2. Onderwijs-deelnemernummer~~	~~een administratienummer dat onderwijsdeelnemers identificeert~~
Nee	~~3. Nationaliteit en geboorteplaats~~	
Nee	~~4. Ouders, voogd~~	~~gegevens bedoeld als 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;~~
Ja, deels	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 handelingsplan - Aanwezigheidsregistratie
Nee	~~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;~~
Nee	~~10. Beeldmateriaal~~	~~foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;~~
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;
Ja	12. Overige gegevens, te weten aspecten van gezondheid	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. - biometrische gegevens - motorische ontwikkeling - sport- en beweegbeleving - sociaal-emotionele ontwikkeling
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

    a. Door Verwerker worden wel/~~geen~~* bijzondere Persoonsgegevens Verwerkt. Het betreft hier de categorieën: 12.

    b. Door Verwerker worden wel/~~geen~~* gevoelige Persoonsgegevens Verwerkt. Het betreft hier de categorieën: 7

    * Doorhalen wat niet van toepassing is.

    De categorieën 3, 5 en 6 zijn bijzondere Persoonsgegevens in de zin van de AVG. De categorieën 7, 9 en 13 worden (in ieder geval) gezien als gevoelige Persoonsgegevens.

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

    Door de de Verwerkers worden geen Persoonsgegevens verwijderd. Onderwijsinstelling is zelf verantwoordelijk voor het verwijderen van deze persoonsgegevens.

    Richtlijnen bewaartermijn persoonsgegevens:

    - Tot 2 jaar nadat de leerling de school heeft verlaten, mogen gegevens bewaard blijven

E. Uitwerking Verwerkingen Persoonsgegevens en doeleinden per product/dienst:

Hieronder wordt per product/dienst van Stimuliz aangegeven op grond van welke van de hierboven genoemde doeleinden en categorieën Persoonsgegevens worden verwerkt.

Product/dienst	**Categorie Persoons-gegevens**	**Toelichting**	**Doelstelling**	**Actief**
Basisadministratie	1, 11	Digitale verwerking van persoonsgegevens die noodzakelijk zijn voor het kunnen werken met het product/dienst.	A, B, C,	X
Gebruikersbeheer	1, 11	Mogelijkheid tot beheer van gebruikers	D	X
Biometrie (optioneel)	1, 7, 12	Afname- en rapportage omgeving voor het digitaal invoeren en bekijken van biometrische gegevens van individuen en groepen.	A, F, G	
Motoriek (optioneel)	1, 7, 12	Afname- en rapportage omgeving voor het digitaal invoeren en bekijken van biometrische gegevens van individuen en groepen.	A, F, G	
Sport- en beweegbeleving (optioneel)	1, 7, 12	Afname- en rapportage omgeving voor het digitaal invoeren en bekijken van gegevens van individuen en groepen over sport- en beweegbeleving.	A, F, G	
Sociaal-emotionele ontwikkeling (optioneel)	1, 7, 12	Afname- en rapportage omgeving voor het digitaal invoeren en bekijken van gegevens van individuen en groepen over sociaal-emotionele ontwikkeling.	A, F, G	

F. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

- Amsterdam, Nederland

G. Subverwerkers

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

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

Naam + vestigingsplaats	**Omschrijving taak/dienst**	**Land van opslag + verwerking**
Digital Ocean, New York, VS	Opslag van data	Nederland / Duitsland
Hello Sunshine	Ontwikkeling online platform	Nederland

H. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij onze supportafdeling via support@stimuliz.com o.v.v. ‘Privacy’.

BIJLAGE 2: Beveiligingsbijlage

1. Beveiligingsmaatregelen en aantoonbaarheid

Stimuliz treft vele technische en organisatorische maatregelen om de veiligheid van de gegevens te waarborgen. De belangrijkste hiervan worden hieronder opgesomd.

a. Voor het classificeren van het product op het gebied van beschikbaarheid, integriteit en betrouwbaarheid is gebruik gemaakt van het Certificeringsschema informatiebeveiliging en privacy ROSA en is te vinden in Bijlage 3.

b. Op basis van het Certificeringsschema informatiebeveiliging en privacy ROSA (https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-v3-0/) worden in het toetsingskader de vereiste beveiligingsmaatregelen voorgeschreven. Stimuliz past de beveiligingsmaatregelen die horen bij de classificatie van Stimuliz toe. De details hiervan zijn te vinden in Bijlage 4. Naast de in het toetsingskader beschreven beveiligingsmaatregelen, past Stimuliz ook de volgende specifieke beveiligingsmaatregelen toe:

    i. De toegang tot persoonsgegevens wordt afgeschermd middels het product 1Password. Hiermee zijn de gegevensdragers beschermd tegen brute force aanvallen, wordt alle toegang tot gegevens gelogd en wordt voor alle gegevensdragers two-factor authenticatie afgedwongen. Ook is hiermee de identificatie, authenticatie en afmelding van medewerkers centraal geregeld;

    ii. Het technische platform is ondergebracht in een hostingcentrum dat 27001:2013 gecertificeerd is.

c. De genomen beveiligingsmaatregelen worden getoetst tegen het toetsingskader van het Certificeringsschema informatiebeveiliging en privacy ROSA. Dit is opgenomen in bijlage 4.

2. Beveiligingsincidenten en/of datalekken

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met de supportafdeling via support@stimuliz.com o.v.v. ‘Beveiliging’.

3. Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

Voor het monitoren en melden van beveiligingsincidenten of datalekken hanteert Stimuliz de volgende procedure:

- Voor het melden en monitoren van beveiligingsincidenten wordt het incidenten-managementsysteem van de servicedesk van Stimuliz gebruikt. In dit systeem krijgen beveiligingsincidenten een aparte categorie waarmee de incidenten gevolgd kunnen worden.

- Beveiligingsincidenten en datalekken kunnen gemeld worden aan de servicedesk middels de gebruikelijke kanalen.

- Stimuliz informeert onderwijsinstellingen over beveiligingsincidenten per e-mail aan de contactpersoon van Stimuliz. Daarbij wordt minimaal de volgende informatie gedeeld:

    - Kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);

- De oorzaak van het incident;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

- In het geval dat het een datalek dat aan de Autoriteit Persoonsgegevens gemeld moet worden, zal Stimuliz contact opnemen met de contactpersoon van de onderwijsinstelling om te bepalen of Verwerker of Verantwoordelijke de melding bij de Autoriteit doet, en of daarvoor alle benodigde informatie aanwezig is.

BIJLAGE 3: Classificatie Certificeringsschema Informatiebeveiliging en Privacy ROSA

Voor het classificeren van het product op het gebied van beschikbaarheid, integriteit en betrouwbaarheid is gebruik gemaakt van het Certificeringsschema informatiebeveiliging en privacy ROSA en is te vinden in Bijlage 3. Deze bijlage geeft een beknopte beschrijving en opsomming van deze classificatie.

1. Beschikbaarheid

Niveau	Omschrijving	Kenmerken
1: Laag	Beschikbaarheid is onbelangrijk. 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.	Beschikbaarheid > 95% RTO= 24-48 uur, afhankelijk van de categorie informatie
2: Midden	Beschikbaarheid is belangrijk. 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.	Beschikbaarheid > 97% RTO= 8-24 uur, afhankelijk van de categorie informatie
3: Hoog	Beschikbaarheid is noodzakelijk. 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.	Beschikbaarheid > 99% RTO= 1-8 uur, afhankelijk van de categorie informatie

Vragen	Niveau	Motivatie
Wanneer moet de dienst beschikbaar zijn voor de gebruikers? - Laag = regulier (bijvoorbeeld alleen kantooruren) - Midden = ruim (bijvoorbeeld 07:00 - 23:00 en/of ook in het weekend) - Hoog = altijd (bijvoorbeeld 24x7)	Laag	Gebruikers zijn actief binnen schooltijden.
Wat is de langste periode dat de ict-toepassing niet beschikbaar mag zijn? - Laag = maximaal enkele dagen - Midden = maximaal een aantal uur - Hoog = maximaal een aantal minuten	Laag	Men kan testen afnemen en op papier invoeren.
Welke impact heeft uitval (de data, informatie of de ict-toepassing zijn niet beschikbaar)? - Laag = geen - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	Laag	Processen kunnen doorgaan. De invoer en verwerking van data kan achteraf plaatsvinden. Er is geen schade geleden.
Op hoeveel gebruikers/organisaties heeft uitval impact? - 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	Laag	Gebruikers gebruiken de applicatie enkele momenten / dagen per jaar.
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? - Laag = nee of verplichtingen langer dan een dag - Midden = er zijn verplichtingen: maximaal een dag onbeschikbaar - Hoog = er zijn verplichtingen: maximaal één uur onbeschikbaar	Laag	Beschikbaarheid naar beste kunnen.

2. Integriteit

Niveau	Omschrijving	Kenmerken
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
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
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

Vragen	Niveau	Motivatie
Kan er misbruik plaatsvinden - bijvoorbeeld fraude met leerresultaten of financiële fraude - door fouten in de gegevens of ongeautoriseerde wijzigingen? - Laag = nee, de gegevens lenen zich niet voor misbruik - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens	Laag	Er worden gegevens verzameld over motoriek en sport- en beweeggedrag. Deze gegevens zijn niet fraudegevoelig.
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	Laag	De gegevens zijn input voor de professional. Deze beoordeelt altijd. Het type adviezen kunnen geen financiële of gezondheidsschade veroorzaken.
Wat is het effect op het onderwijs- of ondersteunend proces als fouten of ongeautoriseerde veranderingen in de gegevens zitten? - Laag = geen - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	Laag	Scholen kiezen ervoor om deze gegevens te verzamelen. Het is geen wettelijke verplichting.
In hoeverre hebben fouten of ongeautoriseerde veranderingen in gegevens invloed op andere toepassingen? - Laag = geen; alleen in de toepassing - Midden = aanzienlijk; ook in andere toepassing(en), door (her)gebruik gegevens. - Hoog = groot effect door bijvoorbeeld automatische beslissingen, veel koppelingen en veel transacties	Laag	De applicatie is niet gelinkt aan andere toepassingen.
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies	Laag	Hier is geen reden voor.
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? - 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)	Laag	Deze zijn er niet en zijn niet noodzakelijk.
Past de toepassing profilering* toe? - 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)	Midden	Op basis van ingevoerde gegevens worden profielen rondom ontwikkeling van motoriek, sport en bewegen opgesteld.
Hoe actueel moeten de gegevens na herstel zijn, totdat dit tot problemen leidt? - Laag = Gegevens mogen enkele dagen oud zijn. - Midden = Gegevens mogen niet ouder dan 24 uur zijn - Hoog = Gegevens mogen niet ouder dan 4 uur zijn	Laag	Gegevens kunnen worden geantidateerd.

3. Vertrouwelijkheid

Niveau	Omschrijving	Kenmerken
1: 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.
2: Midden	Informatie is vertrouwelijk. 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.	Gegevens alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.
3: Hoog	Informatie is geheim. 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.	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.

Vragen	Antwoord	Motivatie
Welke type persoonsgegevens bevat de ict-toepassing? - Laag = geen of 'gewone' persoonsgegevens zoals NAW - Midden = persoonsgegevens als toetsresultaten of gegevens m.b.t. minderjarigen. - Hoog = bijzondere persoonsgegevens, zoals gegevens over etniciteit, politieke opvatting, geloof, gezondheid, seksueel gedrag, etc.	Hoog	Volgens de classificatie van de autoriteit persoonsgegevens vallen de gegevens onder bijzondere persoonsgegevens, namelijk gezondheid.
Leidt openbaarmaking van de gegevens (bv. van examenvragen) of datalek van persoonsgegevens tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies	Midden	Datalek leidt mogelijk tot publieke verontwaardiging.
Kunnen er personen schade ondervinden als gevolg van het uitlekken van de gegevens? - Laag = niet - Midden = ja, maar de gevolgen zijn beperkt - Hoog = ja, fysieke, materiële of immateriële schade. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.	Laag	Een datalek leidt niet tot schade voor de betrokkenen.
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	Hoog	Gegevens worden ingevoerd, verwerkt en bewaard.
Leidt het uitlekken van de gegevens tot economische schade? - Laag = nee - Midden = beperkte economische schade - Hoog = aanzienlijke economische schade	Laag	Een datalek heeft geen economische impact.

* Onder profilering verstaat de AVG "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen" [bron: artikel 4 van de AVG]

4. Uitkomst

Naam project/dienst/document	Stimuliz
Naam Data Classificeerder	G. Van Zeijl
Functie	Functionaris Gegevensbescherming
Datum ingevuld	16 september 2022
Beschikbaarheid	**Laag**
Integriteit	**Midden**
Vertrouwelijkheid	**Hoog**

BIV-Classificatie		
Beschikbaarheid	Integriteit	Vertrouwelijkheid
Laag	Midden	Hoog
Toelichting	Toelichting	Toelichting
Beschikbaarheid is minder belangrijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meer dan een dag brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Integriteit is belangrijk. Blijvende juistheid van informatie is belangrijk, maar sommige toleranties zijn toelaatbaar. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet volledig, correct of actueel is, leidt dit tot substantiële schade.	Informatie is geheim. 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.
Kenmerken	Kenmerken	Kenmerken
Herstel van de dienst mag langer dan 24 uur bedragen.	Bedrijfsproces tolereert een zeer beperkt aantal fouten. Gegevens zijn volledig, juist en actueel; Maximaal toegestaan dataverlies na herstel: 24 uur.	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.

BIJLAGE 4: Toetsingskader Certificeringsschema Informatiebeveiliging

1. Beschikbaarheid

Maatregel	Status en toelichting
Ontwerp	Voldaan
Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals van leveranciers of ketenpartners) en impact van eventuele uitval. Infrastructuur mag bestaan uit: - enkelvoudige applicatieonderdelen - enkelvoudige verbindingen - enkelvoudige aansluiting voeding	*Stimuliz is een op zichzelF staand platform en heeft geen afhankelijkheid met andere systemen.* *Er wordt gebruik gemaakt van gecertificeerde leveranciers en partners.*
Capaciteit beheer	Alternatieve maatregel
De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen.	*Er vindt monitoring van server en storage capaciteit plaats. Bij ontwerp is een inschatting gemaakt van gebruik en resources.*
Onderhoud	Voldaan
Security patches, updates (firmware en software) en vernieuwing van certificaten worden ad hoc uitgevoerd. Urgente security patches worden zo spoedig mogelijk doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	*Security patches, patches t.a.v. server stack (NGINX, PHP, MySQL, Node, NPM) worden automatisch doorgevoerd.* *Dagelijks wordt gecheckt op urgente security patches en waar nodig doorgevoerd.* *Software van derden wordt handmatig up to date gehouden.*
Testen	Voldaan
Onbeschikbaarheid wordt ad-hoc behandeld bv. op basis van een melding van een gebruiker. Beschikbaarheidsincidenten worden geregistreerd.	*Beschikbaarheid wordt gemonitord. Op basis van berichtgeving wordt direct actie ondernomen.*
Monitoring	Voldaan
Terwijl de toepassing wordt gebruikt, wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord.	*Beschikbaarheid wordt gemonitord. Op basis van berichtgeving wordt direct actie ondernomen.*
Herstel	Voldaan
Er is een 'Cold Standby' aanwezig, dat wil zeggen: nieuwe fysieke of virtuele infrastructuur is beschikbaar maar nog niet ingericht. Manueel herstel van de toepassing en gegevens. Recovery test: 1x per 2 jaar. De dienst is in enkele dagen te herstellen.	*Recovery test wordt jaarlijks uitgevoerd en duurt 30 minuten.* *De hostingprovider voorziet in meerdere rekencentra.*

2. Integriteit

Maatregel	Status en toelichting
Herleidbaarheid (gebruikers)	Voldaan
Herleidbaar wanneer, welke gegevens gewijzigd zijn: - Gebruikers hebben standaard (by default) niet meer rechten dan nodig: least privilege - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan maar (indirect) herleidbaar naar personen - Herleidbaar wanneer de gegevens gewijzigd zijn - Gebruikers mogen beheerdersrechten hebben - Wijziging van gegevens is inzichtelijk, zodat een analyse hierop mogelijk is.	*De beheerder van een account bepaald de rechten van gebruikers binnen het account.* *Naamloze gebruikersaccounts zijn niet toegestaan.* *Wijzigingen worden beheerd middels update timestamp.* *Het verwijderen van gegevens worden verwijderen op basis van softdelete.*
Backup	Alternatieve maatregel
Backup is verplicht, minimaal 1 keer per dag, bijvoorbeeld door snapshots. Integriteit van de back-up wordt periodiek (min. 1x per kwartaal) gecontroleerd. Backup wordt beschermd door functiescheiding en fysieke scheiding: opslag op een andere locatie.	*- Backups vinden 1 keer per minuut plaats.* *- Backups worden maandelijks gecontroleerd.* *- Backups worden op fysiek gescheiden locaties bewaard.*
Application controls	Voldaan
Controle op invoer/uitvoer en andere methoden van wijzigen van gegevens: - De toepassing controleert invoer (handmatig of via geautomatiseerde koppeling) door bijvoorbeeld syntax-controle en controle op verplichte velden. In geval van een uploadfunctie, wordt deze beperkt en bestanden worden gecontroleerd. - Uitvoer naar andere systemen wordt opgeschoond tot (veilige) waardes, bv. op basis van syntax-controle. - Foutmeldingen voor gebruikers zijn beperkt; niet meer tonen dan nodig. - Wijzigingen ‘onder water’ (zonder gebruik van de gebruikersinterface) worden als beveiligingsincident opgemerkt en afgehandeld	*Controle op invoer en controle op syntax vindt automatisch plaats.* *Het CI/CD is gericht op het zero-downtime principe middels het blue-green deployments. Dat betekent dat applicatieupdates pas worden gedeployed wanneer deze getest en volledig werkend zijn bevonden.*
Onweerlegbaarheid	Voldaan
Gelogd wordt: inlogactiviteit gebruikers en wijziging van (persoons)gegevens. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken. Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	*Accountactiviteiten worden gelogd op basis van CRUD acties.* *Hierbij wordt zo veel mogelijk aan de richtlijnen van OWASP geconformeerd.* *Logging wordt periodiek gecontroleerd op afwijkende patronen, met name voor toegang tot de applicatie.*
Herleidbaarheid (technisch beheer)	Voldaan
Herleidbaar wanneer, welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn toegestaan en (indirect) herleidbaar naar personen - Herleidbaar wanneer de toepassing gewijzigd is - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen - Toegang met root-accounts is gereguleerd, bijvoorbeeld met expliciete notificatie en logging	*Mutaties van account- en persoonsgegevens worden gelogged. Testgegevens niet.*
Controle integriteit	Voldaan
Periodieke controle integriteit toepassing: - De status van doorgevoerde patches en updates van firmware en software worden periodiek gecontroleerd - Integriteit van de configuratie en software wordt structureel gecontroleerd door een regelmatig uitgevoerd proces Maatregelen tegen malware zijn toegepast Secure software development/secure coding guidelines worden toegepast	*Laravel Forge en Envoyer worden gebruikt om de integriteit van de services te bewaken.* *OWASP is richtlijn voor beveiliging en wordt uitgewerkt in coding guidelines.* *Mallwarebescherming wordt door de hostingpartij verzorgd.*

Onweerlegbaarheid (Toepassing)	Voldaan
Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) De tijd van de applicatie is correct en consistent: wordt gesynchroniseerd met éénzelfde referentietijdbron als aanpalende systemen (binnen een netwerk of organisatie). Deze referentietijdbron is gesynchroniseerd met een publieke tijdsbron. Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	*Logging van technisch beheer wordt uitgevoerd.* *Built en deployment vindt plaats door Gitlab en Envoyer.* *Logging wordt handmatig gecontroleerd.* *Hosting provider verzorgt tijdsynchronisatie. Zij verzorgen server en operating system.*

3. Vertrouwelijkheid

Maatregel	Status en toelichting
Levenscyclus gegevens	Voldaan
Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De applicatie moet het mogelijk maken dat persoonsgegevens verwijderd kunnen worden, bijvoorbeeld op verzoek van de betrokkene. Verwijdering op basis van verstrijken bewaartermijn moet automatisch kunnen. Op media/apparatuur die niet meer worden gebruikt of voor andere doeleinden worden hergebruikt wordt data onherstelbaar vernietigd (bijvoorbeeld degaussing, sanitization, purging, zeroization of vernietiging van de (verwijderbare) media). Output van informatie (zoals een printafdruk) met classificatie vertrouwelijk of geheim dient voorzien te zijn van een label.	*Gegevens kunnen worden ingezien, gedeeld en verwijderd. Op individueel en op groep/klas niveau. School heeft alle middelen en functionaliteiten om de AVG richtlijnen na te leven.* *De verantwoordelijkheid voor het bewaren van data ligt bij de eigenaar van de data.* *Hardware/apparatuur/media wordt door de hostingprovider verwijderd. Deze is ISO 27001 gecertificeerd.* *Output van informatie wordt voorzien van classificatie vertrouwelijk.*
Logische toegang	Voldaan
De toepassing ondersteunt minimaal de volgende maatregelen: - Twee-factor authenticatie (gebruikersnaam en wachtwoord aangevuld met bijvoorbeeld een code op een mobiele telefoon, token of machine certificaat) voor alle gebruikers van de toepassing - Accounts zijn persoonlijk identificeerbaar - Wachtwoordeisen die voldoen aan best practices zoals de richtlijnen van NIST* Er is een geïmplementeerd beleid voor logische toegang (zoals voor supportmedewerkers, beheerders, ontwikkelaars etc.). Daarin zit minimaal een periodieke controle actieve accounts versus actieve medewerkers. En zijn bovenstaande maatregelen van toepassing.	*Twee-factortoegang is optioneel actief.* *Accounts zijn persoonlijk identificeerbaar d.m.v. naam, e-mailadres en organisatie.* *Wachtwoordeisen* *- minimaal 8 karakters* *- numerieke waarde* *- alfanumerieke waarde* *- hoofdletter*
Fysieke toegang	Alternatieve maatregel
Fysieke toegang tot de apparatuur waar de toepassingen en de data verwerkt wordt, is beschermd met minimaal: - Twee factor authenticatie - Logging en monitoring van toegang, bijvoorbeeld cameratoezicht voor de herleidbaarheid. Bezoekers enkel onder begeleiding.	*Apparatuur staat in ISO 27001 (en meer) gecertificeerd rekencentrum.*
Netwerk toegang	Voldaan
Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerksegmentatie, bijvoorbeeld door middel van VLANs - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet en whitelisting van IP-adressen - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	*Servertoegang voor beheerders via geëncrypteerde verbinding en 2FA.* *Toegang tot servers vindt plaats via SSH verbinding.*

Scheiding omgevingen	Voldaan
Ontwikkel, test, acceptatie en productieomgevingen (OTAP) zijn gescheiden. Productiedata (persoonsgegevens, gebruikersnamen, wachtwoorden, et cetera) worden uitsluitend geanonimiseerd gebruikt in ontwikkel- en testomgevingen en waar mogelijk ook in de acceptatieomgevingen. Toegang tot OTAP wordt beheerd en periodiek gecontroleerd en geeft invulling aan de principes 'need to know' en 'least privilege'. Bijvoorbeeld: ontwikkelaars hebben niet standaard toegang tot productieomgevingen. Daarnaast hebben gebruikers standaard geen toegang tot OTA.	*OTAP is volledig gescheiden op applicatie, database en netwerkniveau.* *OTA bevatten geen productiegegevens.*
Transport en fysieke opslag	Voldaan
Encryptie van transport (zowel voor intern als extern verkeer) is conform de Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op twee niveaus, zoals op (virtuele)disk en bestands- of recordniveau. Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	*TLS 1.2 en 1.3 zijn actief* *Encryptie en opslag van data vindt plaats bij een hosting partner die ISO 27001 is gecertificeerd.*
Logging	Niet voldaan
Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen (op basis van autorisatie) en toegang ertoe wordt apart gelogd. Beide logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke patronen in gebruik. Bijvoorbeeld door automatische loganalysetooling.	*Toegang tot de applicatie wordt gelogd, het bekijken van persoonsgegevens niet.* *Logging is enkel toegankelijk op serverniveau. Toegang op serverniveau wordt gelogd. Logging is niet toegankelijk voor beheerders en users binnen organisaties.* *Momenteel vindt enkel handmatige loganalyse plaats.*
Omgaan met kwetsbaarheden	Niet voldaan
Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design en security by design wordt toegepast - Threat modelling - OWASP Top 10 De toepassing wordt getoetst tegen richtlijnen zoals de Uniforme Beveiligingsvoorschriften (UBV) van edustandaard en de NCSC richtlijnen voor webapplicaties. De toepassing wordt periodiek getoetst op passende bescherming van vertrouwelijkheid (minimaal jaarlijks en bij grote wijzigingen), bijvoorbeeld: - Security testen - Vulnerability testen - Pentesten, onafhankelijk door een externe partij Bekende kwetsbaarheden worden adequate opgevolgd (zoals met NCSC beveiligingsadviezen). Indien patches niet aanwezig zijn, worden er alternatieve maatregelen genomen. Inbraakdetectie- en preventiesystemen (IDS/IPS) zijn aanwezig, om aanvallen te detecteren en waar mogelijk automatisch te blokkeren.	*Privacy by design, Threat modeling, OWASP 10, security advisories, throttling van endpoints, security-, vulnerability en pentesten worden toegepast, aangehouden en gemonitord.* *Kwetsbaarheden worden direct opgevolgd.*