Verwerkersovereenkomst 3.0

Deze Verwerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

De nieuwe Verwerkersovereenkomst 3.0 komt in de plaats van eerdere verwerkersovereenkomsten uit 2015 en 2016. De uitgangspunten van deze Verwerkersovereenkomst 3.0 sluiten aan bij de bepalingen in het Convenant, geven invulling aan verplichtingen op grond van de Europese Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals onder andere in (inter)nationale beveiligingsnormen, jurisprudentie en richtsnoeren van de toezichthouder zijn aangegeven.

Deze Verwerkersovereenkomst 3.0 bevat vier bijlagen:

1. In de Privacybijsluiter (Bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
2. In de Beveiligingsbijlage (Bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven
3. Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA"
4. Toelichting op maatregelen "toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA"

Informatie over het Convenant en de model Verwerkersovereenkomst is te vinden op de website www.privacyconvenant.nl. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad, VO-raad, MBO Raad (saMBO-ICT) en bij Kennisnet.

Mei 2018

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 Windkracht Internet B.V. (h.o.d.n. Ziber), gevestigd en kantoorhoudende aan Zijperweg 4 J, te (1742 NE) Schagen, te dezen rechtsgeldig vertegenwoordigd door Maikel Bauer, hierna te noemen: "**Verwerker**"

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

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan voor **Ziber Education**, een communicatieplatform voor kinderopvang en onderwijs, ('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 leerling volgsysteem;

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[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.

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

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. SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS:

   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 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 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 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,
Naam:	Naam: Maikel Bauer
Functie:	Functie: Directeur
Datum:	Datum:

Bijlage 1: Privacybijsluiter
Bijlage 2: Beveiligingsbijlage
Bijlage 3: Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA"
Bijlage 4: Toelichting op maatregelen "toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA"

Bijlage 1- PRIVACYBIJSLUITER GEBRUIK ONDERWIJSCOMMUNICATIEPLATFORM

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.

A. Algemene informatie

Naam product en/of dienst	:	Ziber Education
Naam Verwerker en vestigingsgegevens	:	Windkracht Internet B.V. h.o.d.n. Ziber Zijperweg 4 j 1742 NE Schagen
Link naar leverancier en/of productpagina	:	edu.ziber.nl
Beknopte uitleg en werking product en dienst :		

Ziber Education is een beveiligd digitaal communicatieplatform voor onderwijsinstellingen dat communicatie faciliteert tussen (potentiele) ouders, leerkrachten, kinderen en andere betrokkenen bij de onderwijsinstelling op zowel open als gesloten (beveiligde) wijze. Het platform bestaat onder meer uit websites, apps, webapps, tv schermen, nieuwsbrieven en meer.

De onderwijsinstelling kan informatie delen met ouders, waar ouders vervolgens op kunnen reageren. Ook kan de onderwijsinstelling ervoor kiezen om informatie naar publieke kanalen te publiceren zoals bijvoorbeeld de website of een tv-kanaal (binnen de onderwijsinstelling). Een aantal functies die bijvoorbeeld worden aangeboden zijn; het kunnen plannen van een kind-gesprek, het intekenen door ouders op activiteiten, het kunnen betalen van ouderbijdrage, het tonen van kind-verjaardagen, het delen van foto's met ouders, het contact leggen met ouders of mensen van de onderwijsinstelling.

Als basisgegevens van het Ziber Education platform wordt er eenzijdig gekoppeld met het leerling administratiesysteem van de onderwijsinstelling dan wel kinderopvang (hierna: LAS). Uit het LAS worden de namen van leerlingen, geboortedatum, geslacht, leerjaar en

groepsindeling overgenomen. Ook de namen van leerkrachten en hun groepsindeling wordt overgenomen uit het LAS. Dit gebeurt op basis van een EDEXML (een standaard) of via een directe koppeling met de LAS leverancier. Scholen kunnen dit zonder tussenkomst van derden direct zelf in het Ziber platform verwerken.

Gebruikers van het Ziber platform creëren en beheren zelf een persoonlijk account (Ziber ID), waar zij tenminste een naam en e-mailadres invoeren. Gebruikers kunnen hun persoonlijke Ziber ID vervolgens aanvullen met meer gegevens zoals; geboortedatum, adres, telefoonnummer, geslacht ten behoeve van extra communicatiemogelijkheden.

Doelgroep (zoals po/vo, onderbouw/bovenbouw) : po

Gebruikers : onderwijsdeelnemers/ouders/verzorgers/docenten

B. Omschrijving specifieke diensten

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

Ziber Education platform Bij gebruik van het Ziber Education platform, of een van de onderdelen ervan, maak je gebruik van deze onderliggende verwerkingen:			
Verplichte verwerkingen			
Persoonlijke gegevens (* is verplicht)	Doel	Categorie	Bewaartermijn
Ziber ID (account) Voornaam Achternaam E-mailadres* Geslacht Geboortedatum Adres(sen) Telefoonnummer Profielfoto	1e,2,3,4,5	A,D,K	Ziber ID blijft behouden totdat gebruiker deze wist.
Ouder/verzorger rol Ziber ID	1e	A,D	Ouder/verzorger rol wordt automatisch gewist bij verlaten laatste leerling van deze ouder/verzorger van school en/of zodra Ziber ID wordt gewist.
Leerling rol Ziber ID EDEX-nummer* (administratie) Groep en leerjaar*	1e,2,3,4,5	A,B,G	Leerling rol wordt bij verlaten school gewist. Ziber ID kan door ouder/verzorger worden gewist.
Leerkracht rol Ziber ID EDEX-nummer* (administratie) Groep en leerjaar*	1e,2,3,4,5	A,K	Leerkracht rol wordt, wanneer leerkracht school verlaat, gewist en/of zodra Ziber ID wordt gewist

Beheerder rol Ziber ID	1e,1f,2,3,4,5	A,D,K	Beheerder rol wordt gewist door andere beheerder en/of zodra Ziber ID wordt gewist
Foto's, berichten, evenementen Foto's, berichten en evenementen die tekst, bestanden, beeldmateriaal en/of reacties/aanmeldingen van persoonlijke aard kunnen bevatten	1e	J	Worden automatisch 2 jaar nadat school stopt met het gebruik van Ziber Education gewist.
Optionele verwerkingen			

Ziber Nieuwsbrief			
Verplichte verwerkingen			
Persoonlijke gegevens (* is verplicht)	Doel	Categorie	Bewaartermijn
E-mailadres*	1e,2	A,D	Zolang de gebruiker zich niet zelf heeft afgemeld.
Optionele verwerkingen			

Ziber Pay Bij gebruik van Ziber Pay maak je gebruik van deze onderliggende verwerkingen:			
Verplichte verwerkingen			
Persoonlijke gegevens (* is verplicht)	Doel	Categorie	Bewaartermijn
Transactiegegevens *(Geen bankgegevens)* Het doen van een betaling aan school met een daarbij relevante beschrijving die persoonlijk identificeerbare informatie kan bevatten	1e,1f,2	A,B,G,I	Worden automatisch 2 jaar nadat school stopt met het gebruik van Ziber Education gewist.
Optionele verwerkingen			

De Onderwijsinstelling dient een keuze te maken en daarbij opdracht te geven om persoonsgegevens te verwerken, voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box☐).

De opdracht kan ook worden verleend doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te doen.

C. Doeleinden voor het verwerken van gegevens

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

- ☐ ~~I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of~~

☑ II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

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

1. de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:

   ~~a. de indeling en aanpassing van roosters;~~

   ~~b. de analyse en interpretatie van leerresultaten;~~

   ~~c. het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;~~

   ~~d. het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;~~

   e. de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;

   f. financieel beheer;

   ~~g. 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;~~

   ~~h. het behandelen van geschillen.~~

   ~~i. het uitwisselen van Persoonsgegevens met Derden, waaronder:~~

   ~~j. toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;~~

   ~~k. samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;~~

   ~~l. partijen betrokken bij de invulling van stage of leer-/ werkplekken voor zover noodzakelijk en wettelijk toegestaan;~~

   m. ~~Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.~~

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

3. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
4. 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.
5. 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;
6. ~~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;~~
7. ~~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.~~
8. ~~het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.~~
9. ~~De uitvoering of toepassing van een andere wet~~

D. Categorieën en soorten persoonsgegevens

1. Omschrijving van de categorieën Betrokkenen over wie Persoonsgegevens worden verwerkt, en de categorieën persoonsgegevens van de Betrokkenen:
    a. Contactgegevens - Naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens;
        1. Het geheel aan contactgegevens
        2. Beperkte set = naam, e-mail, opleiding
        3. Persoonlijke set = geboortedatum, geslacht;
    b. Onderwijs-deelnemer-nummer - Een administratienummer dat onderwijsdeelnemers identificeert
    c. ~~Nationaliteit en geboorteplaats~~
    d. Ouders, voogd - gegevens als bedoeld onder a, van de ouders/verzorgers van onderwijsdeelnemers

e. ~~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;~~

f. ~~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;~~

g. 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

h. ~~Onderwijsorganisatie - gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;~~

i. 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;

j. Beeldmateriaal - foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;

k. Docent, zorg-coördinator, intern begeleider, decaan, mentor - gegevens van docenten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;

l. ~~Overige gegevens, te weten .... - andere dan de onder A tot en met K 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.~~

m. ~~BSN/PGN~~

n. ~~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. Door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen): Als beschreven bij B. Omschrijving specifieke diensten.

E. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

Ziber Education platform		
Plaats/Land	Functionaliteit	Verwerkte gegevens
Amsterdam/Nederland	Opslaan en authentiseren gebruikers Verwerking en opslag van foto's, video's en bestanden Verwerking en opslag van gesprekken Versturen van e-mail berichten	Ziber ID en profiel gegevens Foto's, video's, bestanden, groepsberichten, gesprekken, activiteiten

F. Subverwerkers

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

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

Verwerker neemt voor de diensten een Software As s Service (SAAS) licentie af bij Ziber. Daarmee is Ziber feitelijk de enige subverwerker. Ziber maakt op zijn beurt gebruik van de volgende subverwerkers.

Subverwerker en Plaats	Functionaliteit	Verwerkte gegevens
Zendesk, Amsterdam	Het verlenen van support aan de gebruikers Opslaan en authentiseren gebruikers Verwerking en opslag van 1 op 1 gesprekken Verwerken en opslag van tickets en bijlagen	Naam, e-mailadres
Microsoft Office 365, West Europa	Opslag van communicatie en gegevens met onderwijsinstelling	Divers

	waarin persoonlijke gegevens kunnen zitten	
Google	Het meten van het gebruik van het Ziber Education platform ten behoeve functionele verbeteringen	Ip-adres

Opmerking: indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij:

Ziber
Maikel Bauer (m.bauer@ziber.nl)
0224-290989

G. Versie

Versie 3.0 – laatste aanpassing 16 mei 2018

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

Bijlage 2 – BEVEILIGINGSBIJLAGE

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

Minimale beveiligingsmaatregelen en aantoonbaarheid

Op deze plek in de bijlage geven we een verklaring waaruit blijkt dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat:

a. Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;

    1. Zie Bijlage 3 - Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA"

b. Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;

    1. Zie Bijlage 3 - Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA"
    2. Zie Bijlage 4 - Toelichting op maatregelen "toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA"

c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

    1. Zie Bijlage 4 - Toelichting op maatregelen "toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA"

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of Datalek, kan Onderwijsinstelling contact opnemen met: support@ziber.nl of 0224-290996

De contactpersoon voor Verwerker is: [contactgegevens Onderwijsinstelling voor beveiligingsincidenten]

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

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

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,

    - Incidenten die door Verwerker of door derden worden gemeld, worden geregistreerd en geanalyseerd. Uit de analyse kan volgen dat er sprake is geweest van een Datalek en/of een beveiligingsincident.
    - In geval er sprake is geweest van een Datalek worden de getroffen personen in kaart gebracht en om welke data het gaat. Vervolgens wordt informatie over het incident gedeeld als hieronder beschreven.
    - In geval er sprake is geweest van een beveiligingsincident wordt de impact beoordeeld en maatregelen getroffen om dit in de toekomst te voorkomen. Na een aantal vastgestelde maanden worden de genomen maatregelen geëvalueerd.
- De wijze waarop informatie wordt gedeeld;
    - Via telefoon en/of e-mail
    - Gericht aan gebruikers en onderwijsinstelling(en) die het betreft
    - Met Verwerker kan contact worden opgenomen
- Informatie die in ieder geval over een incident gedeeld moet worden
    - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
    - De oorzaak van het beveiligingsincident;
    - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
    - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
    - De omvang van de groep betrokkenen;
    - Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
- Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.
    - Verwerker zal de meldingen naar getroffen personen registreren en dit samen met het incident en procesgegevens melden bij Autoriteit Persoonsgegevens.

Versie: zie onderaan pagina

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

Bijlage 3- Classificatie binnen het Certificeringsschema informatiebeveiliging en privacy ROSA”

Gebaseerd op https://www.edustandaard.nl/app/uploads/2018/02/3._Certificeringsschema_classificatie.xlsx - versie 2.0 , maart 2018

Beschikbaarheid – niveau 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. Kenmerken: RTO*= 1-8 uur, afhankelijk van de categorie informatie				
Vragen	Motivatie	Laag	MIdden	Hoog
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)	Het Ziber platform zou altijd beschikbaar moeten zijn voor de gebruikers, omdat het gebruiksmoment op ieder moment kan zijn.			X
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	Ziber streeft ernaar dat de gehele applicatie altijd beschikbaar is en niet langer dan een paar minuten niet beschikbaar zou zijn.			X
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	Omdat Ziber Education een ondersteunend platform is voor de onderwijsinstelling en geen onderdeel vormt in het primaire onderwijskundig proces, zal de impact voo de school als lastig kunnen worden ervaren maar niet als onoverkomelijk.		X	
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			X	
Zijn er contractuele verplichtingen voor de beschikbaarheid?		X		

- Laag = nee - Midden = ja, er is een standaard SLA of er staan algemene beschikbaarheidseisen in het contract - Hoog = ja, er is een uitgebreide SLA afgedwongen inclusief eisen voor rapportage en responstijd voor incidenten				
Wat is de verwachtte belasting van de ict-toepassing? - Laag = weinig gelijktijdige gebruikers (honderden), weinig transacties (100 per uur), minder dan 1000 requests per seconde - Midden = gelijktijdige gebruikers (duizenden), normale hoeveelheid transacties (100-500 per uur), tussen 1000 en 2000 requests per seconde - Hoog = veel gelijktijdige gebruikers (vele duizenden), veel transacties (meer dan 500 per uur), meer dan 2000 requests per seconde	het Ziber platform bediend zeer veel organisaties en heeft duizenden gebruikers die tegelijkertijd het platform gebruiken.			X

Integriteit – niveau 2 – midden Integriteit is beschermd - Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden. Kenmerken: Een zeer beperkt aantal fouten is toegestaan, Gegevens zijn volledig en juist, RPO* 1 dag				
Vragen	Motivatie	Laag	MIdden	Hoog
Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen? - Laag = nee, de gegevens lenen zich niet voor fraude - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens"	In het Ziber platform worden geen leerresultaten verwerkt en ook niet financiële transacties (wel administratie, maar de daadwerkelijke financiële transactie wordt door een financiële instelling verwerkt).	X		
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan"	Het Ziber platform is een communicatie platform om de communicatie tussen leerkracht en ouders te vereenvoudigen. Ongeautoriseerde veranderingen zullen als lastig worden ervaren door de gebruikers, maar zullen als een laag risico geclassificeerd worden met betrekking tot het primaire onderwijsproces.	X		
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens? - Laag = alleen in de toepassing - Midden = in de toepassing, maar ook in het proces (bijvoorbeeld leerresultaten) - Hoog = groot effect door bijvoorbeeld automatische beslissingen, veel koppelingen en veel transacties"	Fouten of ongeautoriseerde veranderingen in gegevens zullen effect hebben in de toepassing (het zijn van een communicatie platform) maar niet in het primaire onderwijsproces van de onderwijsinstelling.	X		
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies"	Aangezien het Ziber Education platform de communicatie verzorgt tussen school en ouders/verzorgers wordt hiermee ook het imago van de school beïnvloed. Dit kan enige schade opleveren bij ouders (die als klanten dan wel potentiele klanten gezien zouden kunnen worden)		X	
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	Nee, die zijn er niet.	X		

bewijs van werking (denk aan gegevens ten behoeve van bekostiging)"				
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"	De informatie die via het Ziber Education platform met de gebruikers wordt gedeeld is niet van dien aard dat personen er negatieve gevolgen aan zouden kunnen ondervinden. De gegevens worden ook niet gedeeld met andere instanties.	X		

Vertrouwelijkheid – niveau 2 – midden

Informatie is vertrouwelijk, maar niet geheim - 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.

Kenmerken: Gegevens alleen toegankelijk voor directbetrokkenen binnen de organisatie op basis van functie of rol.

Vragen	Motivatie	Laag	Midden	Hoog
Welke type persoonsgegevens bevat de ICT-toepassing? - Laag = geen - Midden = 'gewone' persoonsgegevens zoals NAW - Hoog = bijzondere persoonsgegevens (geloof, medisch, et cetera)"	Het Ziber platform verwerkt alleen gewone persoonsgegevens en niet gegevens zoals bijvoorbeeld 'geloof' of 'medische gegevens' van personen.		X	
Leiden datalekken tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies	Een Datalek van het Ziber platform zou tot kortstondig image verlies kunnen leiden, hoewel dit zou kunnen worden opgevangen door tijdige communicatie. Gezien er geen medische dan wel onderwijskundige informatie gedeeld wordt, kan deze ook niet lekken.		X	
Zijn er contractuele of wettelijke verplichtingen voor de vertrouwelijkheid? - Laag = nee - Midden = ja, deze eisen bescherming - Hoog = ja, deze eisen bescherming, bewijs van werking en melding van inbreuk	Er zijn wettelijke eisen omtrent de vertrouwelijkheid van leerling gegevens.		X	
Kunnen er personen in gevaar worden gebracht als gevolg van het uitlekken van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = personen kunnen het slachtoffer worden van identiteitsfraude"	De gegevens op het Ziber platform zijn alleen NAW-gegevens, waardoor het risico dat personen in gevaar worden gebracht laag is.	X		
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)	Profilering wordt niet gebruikt op het Ziber platform.	X		

Bijlage 4- Toelichting op maatregelen “toetsingskader Certificeringsschema informatiebeveiliging en privacy ROSA”

Gebaseerd op: https://www.edustandaard.nl/app/uploads/2018/02/4._Certificeringsschema_toetsingskader.xlsx - versie 1.2, maart 2018

Beschikbaarheid – niveau 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. Kenmerken: RTO*= 1-8 uur, afhankelijk van de categorie informatie				
Maatregelen	Toelichting	Voldaan / Niet voldaan	Verbeter punten	Planning
Overbelasting	De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om overbelasting te voorkomen. De hoeveelheid gebruikersverkeer wordt automatisch gemonitord en gereguleerd middels load balancers, traffic shapers of een soortgelijke oplossing. Bij overbelasting van het systeem wordt automatisch een notificatie/signalering gestuurd, zodat zo snel mogelijk maatregelen genomen kunnen worden.	Voldaan		
Business continuity	Er is een 'Hot Standby' aanwezig, dat wil zeggen: de toepassing draait reeds op fysieke of virtuele reserve-infrastructuur waar direct naar overgeschakeld kan worden. Bijvoorbeeld door middel van: - active-active applicatieonderdelen - actieve backup netwerkverbinding - UPS/NoBreak Recovery test= 4x per jaar. RTO max= 8 uur. Automatische online failover (verlies van sessies en transacties wordt voorkomen).	Voldaan		
Ontwerp	Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen en impact van eventuele uitval. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om kennisgeving van uitval te geven. Er wordt regelmatig opnieuw geanalyseerd wat de afhankelijkheden met andere toepassingen zijn. Bijvoorbeeld bij grote wijzigingen, aanpassingen of verandering in gebruikersverkeer.	Voldaan		
Monitoring	Terwijl de toepassing wordt gebruikt wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie en herstel van	Gedeeltelijk voldaan	Het proces voor gestructureerd herstel zou als proces beschreven en uitgevoerd kunnen worden.	ntb

	de keten. De cijfers van de recente en huidige beschikbaarheid van de toepassing zijn opvraagbaar voor belanghebbenden.			
Testen	Onbeschikbaarheid en afname van performance direct getest door middel van bijvoorbeeld gebruikssimulaties. Er zijn aantoonbaar proactieve performance testen, bijvoorbeeld bij wijzigingen in ontwerp of verwachtte verandering in gebruikersverkeer.	Gedeeltelijk voldaan	Op het testplatform zouden uitgebreidere performance testen gedaan kunnen worden.	Ntb
Software	Security patches, updates van firmware en software en vernieuwing van certificaten worden met vaste regelmaat in de toepassing uitgevoerd, bijvoorbeeld middels een maandelijks of geautomatiseerd proces. Urgente security patches worden sneller doorgevoerd. Er wordt – waar mogelijk – geautomatiseerd gecontroleerd op security-gerelateerde patches en updates. Software van derden (zoals operating system of libraries) wordt actief onderhouden door de leverancier. Bijvoorbeeld Windows XP wordt niet toegestaan.	Gedeeltelijk voldaan	Het proces van patches en updates doorvoeren is aanwezig maar niet in de vorm van een maandelijks of geautomatiseerd proces wat verbeterd zou kunnen worden.	ntb
Actuele dreigingen (DDoS, ransomware)	Context: voor beschikbaarheid is bijvoorbeeld DDoS een actuele dreiging. De relevante medewerkers zijn op de hoogte van mogelijke bedreigingen. Je bent in staat om spoedig te detecteren of de toepassing niet beschikbaar is door een mogelijke DDoS-aanval. Er is actieve bescherming tegen DDoS-aanvallen, bijvoorbeeld door firewalls of een wasstraat voor internetverkeer.	Voldaan		

Integriteit – niveau 2 – midden

Integriteit is beschermd. - Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.

Kenmerken: Een zeer beperkt aantal fouten is toegestaan, Gegevens zijn volledig en juist, RPO* 1 dag

Maatregelen	Toelichting	Voldaan / Niet voldaan	Verbeter punten	Planning
Integriteit van de gegevens				
Herleidbaarheid (gebruikers)	Herleidbaar wanneer, welke gegevens gewijzigd zijn: - 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 - Toegang en wijziging van gegevens wordt gecontroleerd, bijvoorbeeld met expliciete notificatie aan personen met beheerdersrechten	Gedeeltelijk voldaan	Niet alle wijzigingen zijn terug te draaien en dat vinden wij ook niet wenselijk.	
Backup	Backup verplicht, minimaal dagelijks, bijvoorbeeld door een gescripte backup. RPO max= 1 dag. Restore test= 2x per jaar.	Gedeeltelijk Voldaan	Er wordt niet in een frequentie van 2 x jaarlijks een restore test uitgevoerd	ntb
Application controls	Controle op invoer 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 - Wijzigingen 'onder water' (zonder gebruik van de gebruikersinterface) worden gelogd en de logging wordt periodiek gecontroleerd	Voldaan		

Onweerlegbaarheid	Gelogd wordt: inlogactiviteit gebruikers en wijziging van persoonsgegevens Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Gedeeltelijk voldaan	De logging is aanwezig en wordt op dit moment nog niet periodiek gecontroleerd op afwijkende patronen.	ntb
Integriteit van de toepassing				
Herleidbaarheid (technisch beheer)	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	Voldaan		
Controle integriteit	Periodieke controle integriteit toepassing: - Patchen en updates van firmware en software worden bij grote wijzigingen in de toepassing en handmatig uitgevoerd - Integriteit van de configuratie en software wordt structureel gecontroleerd door een regelmatig uitgevoerd proces Antivirus/malware wordt toegepast Secure software development/secure coding guidelines worden toegepast	Voldaan (waar van toepassing)		
Onweerlegbaarheid	Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Gedeeltelijk voldaan	Logging wordt niet periodiek gecontroleerd op afwijkende patroner	ntb
Actuele dreigingen (DDoS, ransomware)	Voor integriteit is ransomware een actuele dreiging. Houdt rekening met de maatregelen rondom RTO en RPO (bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan 24 uur geleden). Medewerkers worden bewust gemaakt van deze bedreiging en zij daartegen kunnen doen. Bijvoorbeeld netwerkscheiding om propagatie te voorkomen. Je bent in staat om spoedig te detecteren of de (aanpalende) systemen van een toepassing getroffen zijn door ransomware.	Voldaan (waar van toepassing)		

Vertrouwelijkheid – niveau 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.

Kenmerken: Gegevens alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol

Maatregelen	Toelichting	Voldaan / Niet voldaan	Verbeter punten	Planning
Levenscyclus gegevens	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De ict-toepassing moet het mogelijk maken dat persoonsgegevens verwijderd moeten kunnen worden, bijvoorbeeld op verzoek van de betrokkene of wanneer de	Gedeeltelijk voldaan	Wanneer de bewaartermijn is verstreken zou de data automatisch verwijderd kunnen worden	ntb

	bewaartermijn verstreken is. Op media/apparatuur die niet meer worden gebruikt of voor andere doeleinden wordt hergebruikt wordt data gewist én overschreven.			
Logische toegang	Er is een geïmplementeerd beleid voor logische toegang. Daarin zitten minimaal de volgende maatregelen: - Aanvullende authenticatie (gebruikersnaam en wachtwoord en bijvoorbeeld een apart VPN-account of restrictie toegang tot alleen kantoornetwerk) - Accounts zijn persoonlijk identificeerbaar - Een wachtwoordbeleid dat voldoet aan best practices zoals de richtlijnen van NIST* - Periodieke controle actieve accounts versus actieve medewerkers	Voldaan		
Fysieke toegang	Fysieke toegang tot de apparatuur waarop de toepassing draait is beschermd met minimaal: - Eén factor authenticatie - Herleidbaar aan wie de toegang wordt verleend - Bijvoorbeeld middels een gepersonaliseerde toegangspas of persoonlijk token - Logging van toegang Bezoekers enkel onder begeleiding.	Voldaan		
Netwerk toegang	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 geoblocking toepast - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	Voldaan		
Scheiding omgevingen	Ontwikkel, test, acceptatie en productieomgevingen zijn gescheiden. Productiedata (gebruikersnamen, wachtwoorden, et cetera) en persoonsgegevens worden niet gebruikt in ontwikkel- en testomgevingen en waar mogelijk ook niet in acceptatieomgevingen. Testdata zijn altijd geanonimiseerd. Toegang tot productieomgevingen wordt beheerd en periodiek gecontroleerd.	Voldaan		
Transport en fysieke opslag	Encryptie van transport (zowel voor intern als extern verkeer). Encryptie van fysieke opslag. Voor het gebruik van encryptie wordt gebruik gemaakt van richtlijnen/best practices/standaarden. Bijvoorbeeld van NCSC, ENISA, NIST. Daarbij worden de volgende uitgangspunten gehanteerd: - Encryptie welke niet te kraken is binnen de verwachtte levensduur van de versleutelde informatie. - TLS 1.2 of hoger	Gedeeltelijk Voldaan	Encryptie van transport is op alle transport toegepast met de laatst mogelijke techniek. Encryptie voor wat betreft opslag is alleen op high risk informatie toegepast en zou nog breder kunnen worden toegepast zodra de technische standaard dit toelaat.	ntb
Logging	Toegang tot de ict-toepassing en lezen en wijzigen van persoonsgegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen en toegang ertoe wordt apart gelogd.	Gedeeltelijk Voldaan	Lezen en wijzigen van persoonsgegevens valt onder strikte toegangscontrole, maar wordt niet gelogd.	Ntb
Toetsing	Gegevens zijn geclassificeerd. Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design wordt toegepast - Threat modelling - OWASP Top 10	Niet voldaan	Privacy by design wordt toegepast, threat modelling en OWASP top 10 niet.	

	De toepassing wordt getoetst tegen richtlijnen als bijvoorbeeld de NCSC richtlijnen voor webapplicaties.			
Actuele dreigingen (DDoS, ransomware)	Context: Voor vertrouwelijkheid is bijvoorbeeld een hack een actuele dreiging. Medewerkers zijn op de hoogte van mogelijke bedreigingen die leiden tot datalekken, weten hoe ze moeten omgaan met persoonsgegevens en weten waar ze datalekken moeten melden in de organisatie. Je bent in staat om spoedig te detecteren of er een mogelijk datalek is in de toepassing bijvoorbeeld door regelmatige controle van toegangsrechten in de toepassing.	Gedeeltelijk voldaan	Medewerkers zijn op de hoogte van mogelijke dreigingen die leiden tot datalekken. Het detecteren van een mogelijk datalek door middel van controle van toegangsrechten is nog niet toegepast.	ntb