Verwerkersovereenkomst

Ten behoeve van Scholen

April 2018, versie 3

Partijen:

1. Het bevoegd gezag van <naam + rechtsvorm onderwijsinstelling>, <(optioneel) van de scholen genoemd in bijlage 3>, geregistreerd onder bestuursnummer ……/ <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 ThiemeMeulenhoff B.V., gevestigd en kantoorhoudende aan Smallepad 30, te 3811 MG Amersfoort, te dezen rechtsgeldig vertegenwoordigd door Algemeen directeur, de heer H.J.F. Razenberg, hierna te noemen: "**Verwerker**"

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

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij er digitale (cloud) leermiddelen gehanteerd worden en er persoonsgegevens van leerlingen en personeel gebruikt worden conform '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.

Artikel 4: Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens

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

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 door 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 Sub-verwerker

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,

Verwerker,	Onderwijsinstelling,
Datum : ……	Datum : ……
Plaats : Amersfoort	Plaats : ……
Naam : H.J.F. Razenberg	Naam : ……..
Functie : Algemeen directeur	Functie : ……..
Handtekening	Handtekening
……	…….
ThiemeMeulenhoff B.V.	

Bijlage 1: Privacybijsluiter
Bijlage 2: Beveiligingsbijlage
Bijlage 3: (optioneel) overzicht scholenlijst

Bijlage 1

Privacy Bijsluiter
Uitgeverij ThiemeMeulenhoff B.V.

ThiemeMeulenhoff is een educatieve uitgeverij die verschillende digitale producten en diensten (‘**digitale leermiddelen**’) aanbiedt voor gebruik in het primair onderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs en hoger onderwijs, waarbij persoonsgegevens worden verwerkt. Wij vinden het belangrijk om uiterst zorgvuldig met deze persoonsgegevens om te gaan.

ThiemeMeulenhoff heeft het Privacyreglement van haar brancheorganisatie GEU en het ‘Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen’ onderschreven; http://www.geu.nuv.nl/privacy-reglement. In dit convenant is tussen aanbieders en de onderwijssectorraden vastgelegd dat een onderwijsinstelling in juridische zin de ‘verwerkersverantwoordelijke’ is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt. ThiemeMeulenhoff is een ‘verwerker’, die uitvoering geeft aan de opdracht van een onderwijsinstelling.

De afspraken die hiervoor gelden, zijn vastgelegd in de Verwerkersovereenkomst van ThiemeMeulenhoff. Deze Privacy Bijsluiter vormt een onlosmakelijk onderdeel van de Verwerkersovereenkomst. In deze Privacy Bijsluiter richten wij ons tot u als onderwijsinstelling om u meer specifiek te informeren over onze digitale leermiddelen en de bijbehorende gegevensverwerkingen. Daardoor wordt duidelijk welke opdracht u als onderwijsinstelling geeft aan ThiemeMeulenhoff om gegevens te verwerken. Deze Privacy Bijsluiter stelt u tevens in staat om ouders en leerlingen te informeren over de verwerking van persoonsgegevens.

ThiemeMeulenhoff behaalt ISO 27001-certificering voor Information Security Management

ThiemeMeulenhoff, educatieve uitgeverij en een van de grootste producenten van digitale leermiddelen en schoolboeken in Nederland, is sinds 23 december 2017 ISO 27001:2013 gecertificeerd. Met deze belangrijke certificering voor het gebruiken en implementeren van een Information Security Management System (ISMS) kan ThiemeMeulenhoff haar klanten optimale beveiliging van haar informatie garanderen. Met dit certificaat toont ThiemeMeulenhoff aan dat zij voldoet aan de normen van de internationale standaard voor Informatiebeveiliging met haar volledige organisatie, en de ICT-Infrastructuur die zij aan haar klanten levert.

Het ISO 27001-certificaat geeft haar klanten de zekerheid dat ThiemeMeulenhoff beveiliging van informatie beheerst en implementeert, en dat het beleid en de processen op dit gebied continu verbeteren.

A. Algemene informatie

Naam product en/of dienst:	Deze Privacy Bijsluiter ziet op alle digitale leermiddelen die ThiemeMeulenhoff ontwikkelt voor het primair onderwijs, voortgezet onderwijs en beroepsonderwijs. Een transparant overzicht van alle uitgangspunten

	rondom privacy is te vinden op www.thiememeulenhoff.nl/privacy.
Naam Verwerker en vestigingsgegevens:	ThiemeMeulenhoff B.V., Amersfoort. ThiemeMeulenhoff is een aanbieder van (digitale) leermiddelen. ThiemeMeulenhoff heeft zich in de 225 jaar van haar bestaan ontwikkeld tot een ontwerper van eigentijdse onderwijsleerprocessen. ThiemeMeulenhoff werkt vanuit het motto 'Samen leren vernieuwen': om talenten te kunnen laten bloeien, vernieuwt ThiemeMeulenhoff het leren, samen met scholen en docenten. Het bedrijf wil leerlingen laten leren op een manier die bij ze past en die leren leuker maakt. Zo wordt leerrendement verhoogd en meer uit ieder talent gehaald. Met groeiende expertise, ervaring en leeroplossingen is ThiemeMeulenhoff een partner voor scholen in Nederland en daarbuiten bij het vernieuwen en verbeteren van hun onderwijs.
Beknopte uitleg en werking product en dienst:	ThiemeMeulenhoff is een aanbieder van digitale leermiddelen. Binnen deze digitale leermiddelen worden persoonsgegevens verwerkt. Dit zijn bijvoorbeeld de gegevens die leerlingen invullen bij het gebruik van het leermiddel, zoals in een oefenopgaaf of toets. Daardoor is het bijvoorbeeld mogelijk voor leerkrachten om te zien wat ieder van hun leerlingen met de lesstof heeft gedaan en wat het resultaat daarvan is. Om toegang te krijgen tot een digitaal leermiddel moeten gebruikers inloggen. Daarbij worden ook persoonsgegevens verwerkt. Daarnaast is het per instelling mogelijk om te kiezen voor het terugkoppelen van resultaten van het gebruik door leerlingen aan een leerkracht, indien het leermiddel over deze voorziening beschikt. Daardoor is het bijvoorbeeld mogelijk voor leerkrachten om te zien wat ieder van zijn leerlingen met de lesstof heeft gedaan en wat het resultaat daarvan is.
Link naar uitgever en/of privacypagina:	www.thiememeulenhoff.nl, www.thiememeulenhoff.nl/privacy

Doelgroep:	PO, VO, MBO, HO
Gebruikers:	De digitale leermiddelen zijn gericht op gebruik door leerlingen, studenten en docenten, leerkrachten en algemene gebruikers en organisaties en instellingen.

B. Doeleinden voor het verwerken van gegevens en specifieke diensten

ThiemeMeulenhoff maakt een onderscheid tussen verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst, en optionele verwerkingen.

Verwerkingen die een onderdeel vormen van de aangeboden dienst

De verwerkingen door ThiemeMeulenhoff vinden primair plaats om met gebruikmaking van de digitale leermiddelen onderwijs te geven en leerlingen te kunnen volgen en begeleiden.

Bij het gebruik van [Naam product(groep)] vinden altijd de volgende verwerkingen plaats, in lijn met artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen. Voor ThiemeMeulenhoff wordt daaronder verstaan:

Doelen van verwerking

- Identificatie en authenticatie

Voor unieke identificatie en authenticatie van de gebruiker van de producten en diensten van de educatieve oplossing van ThiemeMeulenhoff, om daarmee toegang te verkrijgen tot het betreffende leermiddel.

- Autorisatie

Voor het bepalen van toegang tot de educatieve applicatie en de bijbehorende gebruiksrechten. Hieronder vallen ook de leverings- (ECK) processen welke nodig zijn om een product in gebruik te kunnen nemen.

- Educatieve applicatie functionaliteit diensten

Educatieve applicatie functionaliteit en diensten t.b.v. klant, voor gepersonaliseerde toegang tot de aangeboden diensten; om een applicatie prettig te laten werken wordt functionaliteit aangeboden welke functioneert met een naam en een achternaam. Tevens om adaptief leermateriaal en gepersonaliseerde leerwegen mogelijk te maken, dat is afgestemd op de specifieke leerbehoefte van een gebruiker.

- Opslag van leer- en testresultaten.

Ten behoeve van de opslag en hergebruik van leerresultaten en testresultaten voor de gebruiker.

- Continuïteit en goede werking van het digitale leermiddel.

Borgen van de continuïteit en goede werking van het digitale leermiddel. Waaronder het laten uitvoeren van onderhoud, het maken van back-ups, het aanbrengen van verbeteringen in het leermiddel na geconstateerde fouten en/of onjuistheden, en het verkrijgen van ondersteuning.

- Klassen en leerproces

Ter ondersteuning van het klasse- en leerproces; om bijvoorbeeld leerresultaten van leerlingen aan de leerkracht te kunnen terug koppelen in een resultaten dashboard voor alleen de leerkracht of aan een eventueel leerlingadministratiesysteem (LAS).

- Productontwikkeling en productverbetering

Voor productontwikkeling en productverbetering; hieronder valt ook statistisch onderzoek. Het verwerken van gegevens tot volledig geanonimiseerde onderzoeks- of analysedata ten behoeve van de verbetering van de kwaliteit van onderwijs of productverbetering.

- Gebruiksgegevens en resultaten

Gebruiksgegevens en resultaten. Persoonsgegevens worden alleen verwerkt voor onderwijsdoeleinden, zoals een goede werking van het digitale leermiddel. De gebruiker resultaten worden opgeslagen.

- Adaptiviteit en gepersonaliseerde leerwegen

Om adaptief leermateriaal en gepersonaliseerde leerwegen mogelijk te maken.

- Interne controle

Voor interne controle, beveiliging van de diensten en preventie van misbruik en oneigenlijk gebruik. En het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte persoonsgegevens.

- Support en communicatie

Support en communicatie; Voor het verzenden van elektronische boodschappen over product/diensten van ThiemeMeulenhoff en voor informatie over onderhoud en beheer van de applicatie.

Optionele verwerkingen

Tevens worden door ThiemeMeulenhoff persoonsgegevens verwerkt voor doeleinden waarvoor uiteindelijk specifiek toestemming wordt gevraagd aan de onderwijsinstelling in het kader van:

- het kunnen uitwisselen van leer- en testresultaten aan leerling administratiesystemen van de onderwijsinstelling;

- Het kunnen uitwisselen van leer- en testresultaten en overige statussen zoals voortgang en leerontwikkeling met voorzieningen zoals dashboards welke de onderwijsinstelling in gebruik heeft.

- Extern onderzoek en analyse op basis van de voorwaarden zoals gesteld binnen het ketenplatform van het ‘Convenant Digitale Onderwijsmiddelen en Privacy-Leermiddelen en Toetsen’.

C. Categorieën en soorten persoonsgegevens

De persoonsgegevens die zullen worden verwerkt in het kader van de Service Overeenkomst en haar doeleinden waarvoor ze verwerkt zullen worden.

Categorie van betrokkenen

- Gebruikers
- Leerlingen/Studenten
- Leerkrachten/Docenten
- Onderwijsinstellingen en organisaties

Categorie van gegevens

- Identificatie, onder meer ECKID, basispoortUserID of overige technische of identificerende sleutels om een identiteit te bepalen.
- Voornaam, tussenvoegsel, achternaam
- Schoolinformatie BRIN en ASSU
- E-mailadres
- Gebruiksgegevens en resultaten
- Klassen en leerproces; bijvoorbeeld groep, jaargroep.
- Sociale laag: Persoonlijke en gedeelde notities
- Optimaliseren applicatie en content

Doelen van verwerking

Omschrijving van de doelen van de verwerkte categorieën van persoonsgegevens:

- Identificatie

voor unieke identificatie van de gebruiker van de producten en diensten van de educatieve oplossing. Hierbij wordt gebruikt gemaakt van het ThiemeMeulenhoff authenticatieplatform. Dit zorgt voor een ontkoppeling van het externe id van de school met het interne id van ThiemeMeulenhoff.

Deze unieke identificatie maakt de overige categorieën en verzameldoelen mogelijk.

- Voornaam, tussenvoegsel, achternaam

Voor gepersonaliseerde toegang tot de aangeboden producten en diensten van ThiemeMeulenhoff. Om een applicatie prettig te laten werken wordt functionaliteit aangeboden welke functioneert met een naam en een achternaam. Een gebruiker/docent/leerkracht heeft daarmee overzicht over wie er in een groep zit en welke resultaten er van de gebruiker zijn in het dashboard.

- Emailadres

Support en Communicatie: Het emailadres wordt door ThiemeMeulenhoff gebruikt voor het verzenden van elektronische boodschappen over nieuwe ontwikkelingen t.a.v. het product/de diensten van de educatieve applicatie, voor ondersteuning bij problemen met de dienstverlening, en voor informatie over onderhoud en beheer van de diensten van ThiemeMeulenhoff.

- Gebruiksgegevens en resultaten

Persoonsgegevens worden alleen verwerkt voor onderwijsdoeleinden, zoals een goede werking van het digitale leermiddel. De gebruiker resultaten worden opgeslagen. Daardoor kan een leerkracht bijvoorbeeld in een dashboard zien wat het resultaat is. Denk aan: antwoorden, duur, studieadvies.

Terugkoppelen van resultaten aan docenten en eventueel een leerling administratiesysteem.

Geanonimiseerde informatie voor statisch onderzoek.

- Klassen en leerproces

Binnen de educatieve applicatie zitten (centrale) voorzieningen ter ondersteuning van het klassen- en leerproces.

Denk daarbij aan groepenbeheer, een dashboard met resultaten voor de docent, de mogelijkheid voor de gebruiker om binnen een (gesloten) groep onderling info/notities te maken en te delen.

- Sociale laag: Persoonlijke en gedeelde notities

Er kan in een educatieve applicatie een sociale laag zitten ter ondersteuning van het klasse/ leerproces: Notities zijn persoonlijke tekeningen, prikkers en annotaties die optioneel gedeeld kunnen worden binnen een (gesloten) groep cq klas en daarbuiten, maar alleen binnen de educatieve applicatie.

- Optimaliseren applicatie en content

De persoonsgegevens worden primair verwerkt voor zover deze nodig zijn voor onderwijsdoeleinden, zoals een goede werking van het digitale leermiddel;

ThiemeMeulenhoff kan tevens deze informatie geanonimiseerd gebruiken voor (statisch) onderzoek ter verbetering en optimalisatie van de educatieve applicaties en haar content.

- Schoolinformatie Brin en ASSU

Voor het bepalen van toegang tot de educatieve applicatie en de bijbehorende gebruiksrechten (autorisatie).

Het leggen van een relatie van de gebruiker met de categorie "onderwijsinstellingen en organisaties" ten behoeve van toegang en autorisatie tot de aangeboden diensten en producten van ThiemeMeulenhoff. Tevens voor interne controle, beveiliging van de diensten en fraudepreventie.

In het VO en MBO wordt de identificeren school informatie verstrekt via de IDP/ELO van de school. Houd er rekening mee dat de identificerende schoolinformatie niet altijd correct wordt doorgegeven via de IDP/ELO van de school. Op dat moment zal er eenmalig een interactie met de gebruiker worden gestart om alleen de juiste school te bepalen.

Algemene omschrijving ontvangst attributen uit de keten

Omschrijving van de verwerkte persoonsgegevens in de toegangsketen:	Het verkrijgen van toegang tot digitale leermiddelen verloopt met als beginpunt een Elektronische Leeromgevingen (ELO) of een netwerkleveranciers, of rechtstreeks bij de uitgeverij indien er geen inlogomgeving voorhanden is. Vervolgens loopt deze informatie via één Identity Poviders (IDP) van de school via de Kennisnet federatie, Entree of Basispoort naar de uitgeverij. ThiemeMeulenhoff ontvangt van de diverse partijen attributen op basis waarvan identificatie en autorisatie verzorgt kan worden voor de gebruiker, waarmee vervolgens

	toegang tot het digitale leermiddel wordt gegeven. ThiemeMeulenhoff volgt mede het Edu-k attributenbeleid. Na het inloggen worden door ThiemeMeulenhoff vervolgens de gegevens verwerkt die gebruikers invullen bij het gebruik van het leermiddel, zoals in een oefenopgaaf of toets. Daardoor is het bijvoorbeeld mogelijk voor een leerkracht om te zien wat ieder van zijn leerlingen met de lesstof heeft gedaan en wat het resultaat daarvan is.
Soorten van bijzondere persoonsgegevens:	In onze digitale leermiddelen worden in beginsel geen 'bijzondere categorieën van persoonsgegevens' verwerkt in de zin van artikel 9 van de AVG Leerresultaten en de gegevens van onze (minderjarige) gebruikers beschouwen wij echter als 'gevoelige' gegevens, waarbij wij hogere classificatie eisen stellen aan de betrouwbaarheid, integriteit en veiligheid (BIV) van onze systemen dan aan de publieke sites. De genomen (beveiligings)maatregelen lopen daarin navenant mee.
Bewaartermijn:	ThiemeMeulenhoff verwijdert de verkregen persoonsgegevens conform een schoningsprocedure. De bewaartermijn is daarbij vastgesteld op maximaal 18 maanden. Hierbij is bijvoorbeeld rekening gehouden met eerder opgedane ervaringen vanwege de afwezigheid van gebruikers door bijvoorbeeld ziekte en stages.

D. Algemene informatie over getroffen beveiligingsmaatregelen:

ThiemeMeulenhoff behaalt ISO 27001-certificering voor Information Security Management

ThiemeMeulenhoff, educatieve uitgeverij en een van de grootste producenten van digitale leermiddelen en schoolboeken in Nederland, is sinds 23 december 2017 ISO 27001:2013 gecertificeerd. Met deze belangrijke certificering voor het gebruiken en implementeren van een Information Security Management System (ISMS) kan ThiemeMeulenhoff haar klanten optimale beveiliging van haar informatie garanderen. Met dit certificaat toont ThiemeMeulenhoff aan dat zij voldoet aan de normen van de internationale standaard voor Informatiebeveiliging met haar volledige organisatie, en de ICT-Infrastructuur die zij aan haar klanten levert.

Het ISO 27001-certificaat geeft onze klanten de zekerheid dat ThiemeMeulenhoff beveiliging van informatie beheerst en implementeert, en dat het beleid en de processen op dit gebied continue verbeteren.

Internationale standaard
De ISO 27001:2013-norm is een internationale standaard die eisen specificeert voor het vaststellen, implementeren, uitvoeren, controleren, en bijhouden van een Information Security Management Systeem (ISMS).

Dienstverlening

Doordat er de afgelopen jaren steeds meer informatie wordt uitgewisseld tussen ketenpartijen, in de keten van schoolinstelling tot educatieve uitgeverij, heeft de dienstverlening van ThiemeMeulenhoff behoefte aan een focus op de juiste informatiebeveiliging, waarin het beheersen van risico's en duidelijke communicatie een grote rol spelen.

Een belangrijk onderdeel van het certificeringstraject was het aanleggen van een Information Security Management System, waarin beleid en afspraken rondom informatiebeveiliging centraal beheerd worden. Sleutelwoorden in dit systeem zijn risicobeoordeling, en vaststellen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie.

De certificering maakt het voor ThiemeMeulenhoff mogelijk om de reeds getroffen maatregelen omtrent informatiebeveiliging en security beter te beoordelen. De interne procedures en maatregelen kunnen nu tevens worden beoordeeld door een externe partij die daarbij nieuwe inzichten en eventuele risico's identificeert, waardoor maatregelen en oplossingen worden geboden.

De ThiemeMeulenhoff werknemers en haar partners en leveranciers zijn zich nu veel meer bewust van de risico's omtrent informatiebeveiliging en weten hoe ze op een verantwoorde manier moeten omgaan met bedrijfs- en klant informatie, zowel intern als extern bij de klant.

Geldigheid

De geldigheid van de ISO 27001:2013-certificering van ThiemeMeulenhoff is drie jaar, echter wordt deze jaarlijks door een externe partij opnieuw getoetst om vast te stellen of er een continue verbetering plaatsvindt. Daarnaast blijft ThiemeMeulenhoff eigen initiatieven ontplooien en ontwikkelingen in de markt volgen om daarmee haar informatiebeveiliging verder te optimaliseren.

Voor de toelichting op de genomen veiligheidsmaatregelen verwijzen wij u naar Bijlage 2 van de Verwerkersovereenkomst.

Persoonsgegevens worden door ThiemeMeulenhoff verwerkt binnen Europa. Een overzicht van de opslag en verwerking van subverwerkers die worden ingeschakeld door ThiemeMeulenhoff treft u hieronder.

E. Subverwerkers

Voor bepaalde verwerkingen van persoonsgegevens worden door ThiemeMeulenhoff subverwerkers ingeschakeld.

U kunt hierbij denken aan:

- Ontwikkel- en hostingpartij en haar personeel als verwerker bij haar activiteiten rond applicatie- en technisch beheer van onderdelen van de educatieve applicaties.

- Personeel van ThiemeMeulenhoff en door ThiemeMeulenhoff gecontracteerde partijen die belast zijn met onderhoud en functioneel, applicatie en technisch beheer van de educatieve applicaties.

Als ThiemeMeulenhoff persoonsgegevens laat verwerken door een verwerker, zal ThiemeMeulenhoff er zorg voor dragen dat deze verwerker de gegevens uitsluitend voor de bovengenoemde doelen mag verwerken en voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen. ThiemeMeulenhoff zal met de verwerker een schriftelijke 'verwerkersovereenkomst' sluiten of de overeenkomsten accepteren zoals dit door 'cloudpartijen' wordt gedeponeerd conform de Europese Richtlijnen.

Voor de verwerking van persoonsgegevens worden door ThiemeMeulenhoff subverwerkers ingeschakeld.

Naam:	Omschrijving:	Land van opslag en verwerking:
Sentia, Nieuwegein	Hosting & Beheer en Identity & Access Management	Nederland en Ierland, Europa
iWelcome, Amersfoort	Identity & Access Management	Ierland, Europa
Trifork, Amsterdam	Databasemanagement en externe koppelingen	Nederland
Centric, Deventer	Ontwikkeling & Beheer	AWS, Centric Roemenië
Dsens, Amsterdam	Ontwikkeling & Beheer	Nederland
ICATT, Amsterdam	Ontwikkeling & Beheer	Nederland
Uniserver Internet B.V., Alkmaar	Hosting	Nederland
Enigmatry, Rotterdam	Ontwikkeling & Beheer & Hosting	Alleen voor NT2, Europa
Zest Software, Rotterdam	Ontwikkeling & Beheer	Nederland
BloomReach B.V, Amsterdam	Ontwikkeling & Beheer	Nederland
LeaseWeb Netherlands B.V., Amsterdam-Zuidoost	Hosting	Nederland
Usabilla, Amsterdam	Informatiemeldingen op sites	Ierland, Europa
Microsoft Azure, Schiphol Rijk	Hosting	Ierland, Europa
Amazone Web Services AWS, Den Haag	Hosting	Ierland, Europa
Valtech, Amersfoort	Corporate site & Webshop	Ierland, Europa
Youwe, Groningen	Webshop	Frankfurt, Duitsland
ASSU, Groningen	Scholen en docentenregistratie tbv validatie aankoop en nieuwsbrieven.	Nederland

F. Regeling inzage- en correctierecht ThiemeMeulenhoff

De regeling inzage en correctierecht ThiemeMeulenhoff, zie www.thiememeulenhoff.nl/privacy, geldt wanneer betrokkenen (leerlingen, docenten, gebruikers, ouders en andere wettelijke vertegenwoordigers) verzoeken om inzage in de persoonsgegevens die verwerkt worden door ThiemeMeulenhoff in haar rol als verwerker maar ook als verwerkingsverantwoordelijke conform de bepalingen in de Algemene Verordering Gegevensbescherming.

ThiemeMeulenhoff onderschrijft het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen. In convenant tussen aanbieders en de onderwijssectorraden is vastgelegd dat een onderwijsinstelling in juridische zin de 'verwerkingsverantwoordelijke' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt.

Bovenstaande betekent dat leerlingen, ouders of wettelijke vertegenwoordigers die contact opnemen met uitgeverij ThiemeMeulenhoff omtrent een inzage of correctieverzoek zullen worden doorverwezen naar de verantwoordelijke van de persoonsgegevens: de onderwijsinstelling.

Met deze privacy bijsluiter heeft u als onderwijsinstelling inzage in de persoonsgegevens die ThiemeMeulenhoff over uw kinderen heeft vastgelegd en kunt u dat verantwoorden.

Wanneer ThiemeMeulenhoff stopt met het verwerken van gegevens van uw kinderen, dan houdt dat in, dat de school uw kinderen niet meer persoonlijk kan laten inloggen en via de computer of tablet kan laten oefenen met lesstof en oefenopgaven van ThiemeMeulenhoff.

Als u als school in opdracht van een ouder of wettelijke vertegenwoordiger wilt dat ThiemeMeulenhoff stopt met verwerken van gegevens van een specifieke leerling, dan verzoeken wij u per e-mail contact opnemen met ThiemeMeulenhoff via privacy@thiememeulenhoff.nl, met alle relevante informatie, inclusief een bewijs van inschrijving van de betreffende leerling op uw school.

ThiemeMeulenhoff zal in uw opdracht de persoonsgegevens van het specifieke kind zo spoedig mogelijk binnen haar mogelijkheden proberen te verwijderen.

G. Contactgegevens

Voor vragen of opmerkingen over deze Privacy Bijsluiter of de werking van onze digitale leermiddelen, kunt u terecht bij: ThiemeMeulenhoff, t.a.v. Security Manager, Postbus 400, 3811 MG, Amersfoort. Onze helpdesk is telefonisch bereikbaar. Alle actuele contactinformatie vindt u op www.thiememeulenhoff.nl/contact.

H. Versie

Deze Privacy Bijsluiter is voor het laatst bijgewerkt op 1 april 2018.

Deze privacy bijsluiter 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://ww.privacyconvenant.nl.

Bijlage 2

Technische en organisatorische beveiligingsmaatregelen

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

ThiemeMeulenhoff neemt passende technische en organisatorische maatregelen om de persoonsgegevens van uw leerlingen te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking

I. Maatregelen om persoonsgegevens te beschermen

Organisatie van informatiebeveiliging en communicatieprocessen

- ThiemeMeulenhoff is sinds 23 december 2017 ISO 27001:2013 gecertificeerd.

  De ISO 27001:2013-norm is een internationale standaard die eisen specificeert voor het vaststellen, implementeren, uitvoeren, controleren, en bijhouden van een Information Security Management Systeem (ISMS).

- ThiemeMeulenhoff heeft een informatie security management systeem (ISMS). Daarin is een informatiebeveiligingsbeleid vastgesteld, en organisatorisch een Security Manager aangewezen, inclusief security officers, om risico's omtrent te verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.

- Jaarlijks ondergaat ThiemeMeulenhoff een interne audit uitgevoerd door de ISMS organisatie. En daarnaast is er jaarlijks een externe audit op de ISMS processen door de ISO certificerende partij.

- Informatiebeveiliging is binnen ThiemeMeulenhoff als een proces ingericht. Dat betekent dat voor elke maatregel documentatie wordt vastgelegd en wordt onderhouden.

- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.

- ThiemeMeulenhoff heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

- Alle medewerkers van ThiemeMeulenhoff hebben awareness training gehad omtrent informatiebeveiliging.

- Periodiek worden er nieuwe prioriteiten gesteld t.a.v. optimaliseren en verbeteren van beleid, volgens de Plan, Do, Check, Act cyclus.

- Ontwikkelingen in het veld van privacy en security worden gevolgd. Hieronder valt ook bijvoorbeeld: de Algemene Verordening Gegevensbescherming (Europese Verordening Dataprotectie) en de richtsnoeren van de Autoriteit Persoonsgegeven, en betrokkenheid van EDU-K en de GEU rondom het Convenant Digitale Onderwijsmiddelen en Privacy.

Personeel en leveranciers

- Met leveranciers en personeel zijn en worden geheimhoudingsverklaringen overeengekomen en worden verwerkersovereenkomsten en informatiebeveiligingsafspraken gemaakt.
- ThiemeMeulenhoff stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.
- ThiemeMeulenhoff beschikt over beleid omtrent de beveiliging van en de omgang met persoonsgegevens en het gebruik van media en netwerkdiensten door personeel en leveranciers.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

  Enkele voorbeelden ter onderbouwing:

Medewerkers en gegevens:	Handelingen:
Medewerkers van de klantenservice hebben toegang tot licentieinformatie. Zij kunnen onder meer zien voor welke leerlingen een digitaal leermiddel is geactiveerd.	Administratieve handelingen in het kader van de werking van leermiddelen en licenties. Ondersteuning van de eindgebruiker. De klantenservice heeft geen inzage in leerresultaten van leerlingen.
Analisten / deskundigen op het gebied van ontwikkeling van lesmateriaal hebben toegang tot geanonimiseerde sets van resultaten van gebruik van leermiddelen, eventuele problemen/fouten bij gebruik	Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van adaptief lesmateriaal, opsporing en verbetering van fouten in de werking van het digitale leermiddel.
IT-databasebeheerders hebben toegang tot de databases.	De handelingen van IT-databasebeheerders zijn gericht op continuïteit en optimalisatie van ICT-systemen.

Fysieke beveiliging en continuïteit van de middelen

- Er wordt steeds meer gewerkt met ISO27001/27002 gecertificeerde leveranciers.
- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.

- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.

- Er worden backups gemaakt om de continuïteit van de dienstverlening te verzekeren.

Netwerk-, server- en applicatiebeveiliging en onderhoud

- Gegevens die binnen applicaties worden verwerkt zijn geclassificeerd op risico's.

- De netwerkomgeving waarbinnen gegevens worden verwerkt is beveiligd door o.m. proxy's en firewalls. Daarbij worden maatregelen geïmplementeerd tegen misbruik en aanvallen.

- Applicatieleveranciers en ontwikkelaars krijgen instructie t.a.v. (secure) applicatie development, op basis van o.m. OWASP standaarden.

- De omgevingen waarbinnen persoonsgegevens worden verwerkt worden gemonitord.

- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd onder regie van een changemanager.

- Penetratietests en vulnerability assessments worden uitgevoerd al naar gelang de lifecycle situatie van de applicatie, de classificatie van de applicatie en haar data, en haar rol in de keten.

- Er wordt gebruikgemaakt van versleutelde verbindingen voor de uitwisseling van gegevens en inlogprocessen.

Beveiliging en continuïteit van de middelen, het netwerk, de server en de applicatie conform het Certificeringsschema

- Onderstaande rapportage geeft een overzicht van de maatregelen conform het Certificeringsschema. De ISO 27001 is uitgebreider en ook essentiëler, want is mede gericht op de medewerkers en haar processen i.t.t. het certificeringsschema.

  ThiemeMeulenhoff gebruikt de ISO 27001:2013-norm als haar standaard voor het beoordelen van het Information Security Management Systeem (ISMS), met als doel het creëren van een solide basisniveau van informatiebeveiliging en privacy.

- ThiemeMeulenhoff gebruikt het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/) als inzichtelijk en transparant kader in de communicatie naar schoolinstellingen en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor ThiemeMeulenhoff.

- Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Generiek gezien is er een basisniveau vastgesteld.

Toetsvorm	Jaarlijks Interne audit en externe audit conform ISO 27001:2013 norm, Certificaat Nr.: 248549-2017-AIS-NLD-UKAS

Uitvoerder toets	Interne audit, ThiemeMeulenhoff & Northwave, CISO Externe audit, DNV. GL, Londen, Auditor		
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=3, TLP=ROOD ThiemeMeulenhoff hanteert haar interne classificatie op basis 0,1,2.		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
		[Voldaan/ niet voldaan/ alternatieve maatregel]	[Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven]
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Voldaan	
	Actuele dreigingen	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	
	Backup	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Actuele dreigingen	Voldaan	
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Voldaan	
	Toetsing	Voldaan	
	Actuele dreigingen	Voldaan	

Rapportage

Verwerker rapporteert aan ThiemeMeulenhoff over updates of beveiligingsincidenten. De verwerker actualiseert de informatie en informeert contractpartijen en/of gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen.

De ThiemeMeulenhoff security officers rapporteren vervolgens aan de Security Manager, t.b.v. het ISMS overleg.

ThiemeMeulenhoff communiceert haar maatregelen rondom de technische en organisatorische maatrelen jaarlijks via de privacybijsluiter. De intentie is om dit samen met de aanschaf van het producten te laten verstrekken (door distributeur). Hierdoor is er geen aparte administratie benodigd t.a.v. verwerkersovereenkomst en privacy bijsluiter en zal de administratieve belasting voor de school en de uitgeverij idealiter minimaal zijn.

Omdat er sprake is van een continue ontwikkelproces rondom de informatiebeveiliging, idealiter naar een hoger en beter niveau, worden updates rondom de privacybijsluiter weergegeven op www.thiememeulenhoff.nl/privacy. De status kunt u achterhalen op basis van de versiedatum.

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van ThiemeMeulenhoff, www.thiememeulenhoff.nl/contact of een e-mail te sturen naar privacy@thiememeulenhoff.nl.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

ThiemeMeulenhoff heeft een Incident en Response Procedure ingericht.

- *De wijze waarop monitoring en identificatie van Datalekken plaatsvindt*

ThiemeMeulenhoff monitort haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een Datalek worden beoordeeld door het ISMS proces, onder verantwoordelijkheid van de security manager van ThiemeMeulenhoff, die analyseert of sprake kan zijn van een Datalek.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een Datalek voordoet, wordt de verantwoordelijke onderwijsinstelling door of namens ThiemeMeulenhoff in beginsel binnen binnen 24 uur na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens, of via een nader te bepalen instructie die centraal gecommuniceerd zal worden in het geval van een calamiteit.

- *ThiemeMeulenhoff deelt ten minste de volgende informatie wanneer zich een Datalek voordoet:*

    - 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).

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

Versie

Deze bijlage is voor het laatst bijgewerkt op 1 april 2018.

Deze bijlage 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://ww.privacyconvenant.nl.

BIJLAGE 3: Scholenlijst

BRIN	Schoolnaam	Adres	Postcode en woonplaats