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 beroeps onderwijs 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 onze klanten de zekerheid dat ThiemeMeulenhoff beveiliging van informatie beheerst en implementeert, en dat het beleid en de processen op dit gebied continue 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 erbuiten 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 een leerkracht om te zien wat ieder van zijn 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 een leerkracht 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, ondermeer ECKID, basispoortUserID of overige technische of identificerende sleutels om een identiteit te bepalen.
- Voornaam, tussenvoegsel, achternaam
- Schoolinformatie Brin en ASSU
- Emailadres
- 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 categorieen 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

Beveiligingsbijlage: 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 organasatie. 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 Verordering 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.