BIV en PIA online leren

IBPDOC17

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie

Kennisnet / saMBO-ICT

Auteurs

Marc Dietzenbacher (ROC Leeuwenborgh)
Maurits Toet (Cerrix)
Ludo Cuijpers (ROC Leeuwenborgh)
Leo Bakker (Kennisnet)

Versie 1.0 juli 2016

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding en procesbeschrijving

1.1 Aanleiding

Binnen het mbo onderwijs wordt steeds meer gebruik gemaakt van digitaal educatief leermateriaal. Dit brengt veel uitdagingen met zich mee, met name op het gebied van bestellen, installeren dan wel toegang verlenen en gebruiken. Dit document beschrijft hoe een mbo instelling deze zaken praktisch kan benaderen en op basis daarvan een adequate BIV classificatie en een privacy impact assessment (PIA) gemaakt kan worden. In dit hoofdstuk wordt kort die praktische aanpak beschreven aan de hand van de processen en worden de ook de risico's beschreven.
In het tweede hoofdstuk wordt ingegaan op de gehanteerde dataset en derde hoofdstuk behandelt de BIV classificatie. In hoofdstuk 4 wordt tenslotte de PIA beschreven. In de bijlagen wordt een voorbeeld bewerkersovereenkomst weergegeven, alsmede het overzicht van het gehele framework ibp voor het mbo.

1.2 Globale procesbeschrijving

Binnen een mbo instellingen zijn er niet altijd formeel vastgestelde procesbeschrijvingen in het kader van de aankoop en gebruik van digitale applicaties. De onderwijssectoren mogen vaak zelf de keuze maken of ze wel of niet met distributeurs in zee gaan. Een tweetal voorbeelden:

- De docenten van de sector Zorg en Welzijn stellen de boekenlijst vast en vervolgens wordt deze (digitaal) verzonden naar de studenten. De studenten bepalen dan zelf of ze in zee gaan met een distributeur, een internetwinkel of een lokale boekhandel.
- De docenten van de sector Techniek stellen de boekenlijst vast en laten de bestelling volledig verzorgen door een distributeur.

Beide opties hebben voor- en nadelen die echter onvoldoende zwaar wegen om van de ingeslagen weg af te wijken. Problemen ontstaan met name als ouders de bestelling regelen en vervolgens de account gegevens ontvangen en niet doorgeven aan hun zoon of dochter. Dat is een frequent terugkerend probleem. Dan dringt zich de keuze op om een meer centraal geleid proces in te richten om bestellen van, toegang tot en gebruik van digitaal educatief leermateriaal goed te laten verlopen, daarbij gebruik makende van een federatieve toegang waarbij het mbo instellingaccount leidend is.

Daarbij wordt een mbo instelling dan geconfronteerd met een drietal opties waaruit een keuze gemaakt moet worden.

- Allereerst gaan is er de vraag of de instelling aan de slag gaat met een Federatieve inlog (Kennisnet Federatie of SURFconnext)
- Gaat de instelling gebruik maken van de UPN (User Principal Name), in de vorm van studentennummer + domeinnaam (zie volgend hoofdstuk).
- Gaat de instelling werken volgens het principe van IDP first (de basis gegevens ingevuld door de mbo instelling en de student geeft akkoord) of IDP last (de student logt in bij de leverancier met een account en dit wordt pas later gekoppeld met het mbo instellingaccount)[1].

1.3 Risico's

Er zijn een aantal issues die een goed verloop van deze keten kunnen verstoren. Als de mbo instelling kiest voor IDP first, hetgeen de meeste voordelen biedt, moet er wel rekening gehouden worden met de noodzaak om het ID-management heel goed op orde te hebben. De student moet in een vroeg stadium over zijn of haar mbo instelling account kunnen beschikken. Soms wordt daarom min of meer noodgedwongen overgegaan op IDP last, waar bij de koppeling met het mbo instellingaccount in een later stadium plaatsvind. Ook daar zijn risico's aan verbonden.
Vervolgens moeten er in beide gevallen goede afspraken gemaakt worden met de distributeurs en applicatie leveranciers.

[1] Meer informatie over deze processen kan via het iECK project bij Kennisnet worden opgevraagd.

Kennisnet heeft hiertoe het voortouw genomen met name op het gebied van Bewerkersovereenkomsten en het Edustandaard Certificeringsschema.
In het geval dat de mbo instelling de gegevens direct aan de leverancier aanlevert moet er ook een bewerkersovereenkomst met de leverancier zijn afgesloten. Maar ook bij IDP last wordt bij de achteraf koppeling met het mbo instellingaccount een dergelijke overeenkomst noodzakelijk geacht. Bij gebruik van de educatieve software is er bijna altijd sprake van bewerking van gegevens (groepindeling, interactief materiaal, voortgang van de student) zodat er altijd een bewerkersovereenkomst afgesloten moet worden.
Wel is het zo dat er nog volop gesproken wordt over rollen en verantwoordelijkheden van de onderwijsinstelling, distributeur en applicatieleverancier bij de verstrekken van aanvullende gegevens en het gebruik van de educatieve software. Een collectieve afspraak hierover tussen de scholen (MBO Raad, saMBO-ICT) en leveranciers (diverse koepelorganisaties) is wenselijk maar als zodanig nog niet gerealiseerd.

2. Dataset online leren

2.1 Dataset die doorgegeven wordt aan online aanbieders

De mbo instelling maakt gebruik van de diensten van de Kennisnet Federatie (vroeger Entree). Door de "*Bijlage bij Aansluitvoorwaarden Kennisnet Federatie Identity Provider*" te tekenen gaat de mbo instelling ermee akkoord dat de volgende gegevens worden doorgegeven aan derden:

Attribuutnaam	**Omschrijving**
nlEduPersonProfileId	Unieke gebruikersID binnen de mbo instelling: studentnummer@administratie.mbo instellingdomein
FirstName	Naam: Voornaam
nlEduPersonTussenvoegsels	Naam: Tussenvoegsels
Sn	Naam: Achternaam
Attributen ten behoeve van groepering in de educatieve applicaties	
EduPersonAffiliation	Rol (student/docent/beheerder, default=student)
nlEduPersonUnit	Primaire klas/groep (**bijv. H2A**). Uniek binnen administratie.mbo instellingdomein
nlEduPersonDepartment	Vestiging
Attributen ten behoeve van herkenning van de boekenlijsten	
nlEduPersonCohort	Startjaar (**bijv. 2014**)
nlEduPersonProfile	Opleidingsnaam voorafgegaan door CREBO<spatie> **(bijv 2345 ICT.Gamedeveloper).** Indien er sprake is van BOL of BBL, mogen die OPTIONEEL toegevoegd worden als BOL_ of BBL_ voor de opleidingsnaam **(bijv 2345 BOL_ICT.Gamedeveloper)**
ocwILTLeerjaar	Leerjaar

Deze gegevens worden door Entree pas doorgegeven nadat de mbo instelling daar allereerst nadrukkelijk toestemming toe heeft gegeven. Deze toestemming wordt door Entree als volgt verwoord:

… Entree geeft uit privacy overweging een andere, versleutelde inlognaam door aan de dienst-aanbieders (service providers) die via de Entree Federatie bereikbaar zijn. Door deze versleuteling zijn de eindgebruikers (studenten) providers niet individueel traceerbaar.
De dienst-aanbieder waarbij u diensten (digitale content) afneemt of wil gaan afnemen, wil voor haar dienstverlening aan u gebruik maken van extra attributen. Dit is noodzakelijk om bijvoorbeeld per student een leerplan bij te houden of om specifiek onderwijsmateriaal aan te bieden. Door deze extra attributen kan de eindgebruiker mogelijk individueel traceerbaar worden bij de dienst-aanbieder. Entree is volgens haar voorwaarden niet zondermeer bevoegd deze privacy gevoelige informatie door te geven. De gebruiker (de mbo instelling; identity provider) dient hiervoor expliciet toestemming te geven middels dit formulier. ..

2.2 Deelnemende aanbieders

Onderstaan online aanbieders van digitaal lesmateriaal nemen deel aan het Kennisnet (Entree) initiatief:

- Studystore, Emmen
- Lisette Werter Groep
- van Dijk Educatie, Kampen
- Studieboekencentrale, Emmen
- Eduroute (via Ultraware, Assen)
- Uitgeverij Malmberg, 's-Hertogenbosch
- Thieme Meulenhoff, Amersfoort
- Noordhoff Uitgevers, Groningen
- Uitgeverij Deviant, Amersfoort

- Edu' Actief, Meppel
- Stichting Praktijkleren, Amersfoort
- IT Workz (product Stimmit), Etten-Leur

Intussen kunnen ook andere, nog niet benoemde leveranciers deel nemen aan dit initiatief.

3. BIV classificatie

De BIV classificatie bestaat uit drie onderdelen te weten beschikbaarheid, integriteit en vertrouwelijkheid. Het document Handboek BIV classificatie (IBPDOC14) is onderdeel van het mbo framework en daarin worden de naast de definities van beschikbaarheid, integriteit en vertrouwelijkheid ook de classificatie indelingen in drie klassen weergegeven: laag, midden en hoog. Het is van belang deze klassenindeling met bijbehorende beschrijving en beheersmaatregelen voor alle processen toe te passen zodat er van uniformiteit gesproken kan worden. Deze indeling komt ook weer terug in de afspraken kaders die met leveranciers worden gehanteerd. Het staat de instelling uiteraard altijd vrij om daar een eigen invulling aan te geven.

3.1 Beschikbaarheid

Beschikbaarheid is een kwaliteitscriterium dat als volgt wordt gedefinieerd:
De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is.
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is.
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

De classificatie indeling is Laag, Midden en Hoog zoals uitgewerkt in de volgende tabel:

	Classificatie Indeling	**Classificatie gevolg**	**Beheersmaatregel**
Beschikbaarheid	Beschikbaarheid **Laag**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Beschikbaarheid netwerk standaard. • Standaard back up en restore test
	Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur**[2] brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Beschikbaarheid netwerk standaard. • Regelmatig back up en restore test • Risico analyse op de keten uitgevoerd (zie voorbeeld) • Reserve onderdelen voor MER en SER aanwezig
	Beschikbaarheid **Hoog**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **4 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Standaard netwerk plus extern netwerk • Regelmatig back up en restore test • Extern netwerk beschikbaar

[2] ho: 24 uur

3.2 Integriteit

Integriteit is een kwaliteitscriterium dat als volgt wordt gedefinieerd:
De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de it-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in it-systemen ten opzichte van de werkelijkheid is gewaarborgd.
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is.
- Waarborging: de mate waarin de correcte werking van de it-processen is gewaarborgd.

In de onderstaande tabel is per classificatie indeling het classificatiegevolg beschreven met de daarbij behoren beheersmaatregel.

	Classificatie indeling	**Classificatie gevolg**	**Beheersmaatregel**
Integriteit	Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	• Application controls + business rules
	Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	• Application controls + business rules • Manual controls
	Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	• Application controls + business rules • Manual controls • 4 ogen principe

3.3 Vertrouwelijkheid

Vertrouwelijkheid is een kwaliteitscriterium dat als volgt wordt gedefinieerd: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is.
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is.
- Identificatie: de mate waarin mechanismen ter herkenning van personen/apparatuur gewaarborgd zijn.
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

	Classificatie indeling	**Classificatie gevolg**	**Beheersmaatregel**
Vertrouwelijkheid	Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of studenten. Vertrouwelijkheid is gering.	• Generieke toegangsbeveiliging
	Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	• Autorisatiematrix
	Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	• Autorisatiematrix • Eventueel aanvullende maatregelen zoals 2-weg authenticatie[3] en/of encryptie[4]

[3] 2-weg authenticatie: medewerkers kunnen alleen inloggen nadat ze twee handelingen hebben uitgevoerd. Bijvoorbeeld nadat ze zijn ingelogd moet er ook nog een code worden ingevoerd die per sms is toegezonden.
[4] Encryptie: informatie is versleuteld en kan alleen door een aangewezen ontvanger worden gelezen.

3.4 Online leren classificatie

Uitgaande van deze generieke beschrijvingen vanuit het handboek BIV classificatie is het zaak om dit toe te passen op het proces digitaal educatief leermateriaal, in de wandelgang hier ook wel online leren genaamd vanwege het feit dat je via het internet toegang tot deze materialen krijgt en meestal in de cloud aan het werk bent.

Beschikbaarheid: als uitgangspunt voor de processen rond digitaal educatief leermateriaal wordt voor beschikbaarheid de klasse **MIDDEN** gekozen. Dit lijkt voor het gebruik voor de student een voldoende garantie om te kunnen werken en het is voor mbo instelling en leverancier ook een haalbaar criterium. Dit is ook met de leveranciers afgestemd.

Integriteit: het is belangrijk dat de juiste student toegang krijgt tot de juist online educatieve content. Het is echter niet nodig om de data dubbel te controleren (4 ogen principe). Dit leidt ertoe dat voor de processen rond digitaal educatief leermateriaal voor een integriteitsclassificatie **MIDDEN** is gekozen.

Vertrouwelijkheid: de classificatie midden duidt op de informatie die gekoppeld is aan een rol van een medewerker of de opleiding van een student. Hier valt ook de informatie onder die persoonsgebonden is, zoals e-mail. Apart inloggen is noodzakelijk. Uiteraard kan dit vereenvoudigd zijn doordat er gebruik gemaakt wordt van een Single Sign On methodiek. Het is daarom vanzelfsprekend dat ook voor vertrouwelijkheid de klasse **MIDDEN** als standaard is gekozen. Dit is ook een logische keuze omdat er geen zeer privacy gevoelige informatie wordt gedeeld zoals in zorgdossiers e.d..

Op basis van de wensen, de financiële mogelijkheden en bovenstaande argumentatie wordt “Online leren” gelabeld, op basis van de vastgestelde BIV classificatie, met M-M-M. Schematisch als volgt weergegeven.

Proces: **Online leren**	**29**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)*

4. Privacy Impact Assessment

4.1 Inleiding

Tweede stap in de procesbenadering is het doen van een privacy impact assessment (PIA). In goed Nederlands is dat een gegevensbeschermingseffectbeoordeling (gbeb). In het toetsingskader privacy in het mbo (IBPDOC7) is dit bij statement P21 uitvoerig weergegeven:

P21 MBO controledoelstelling: gegevensbeschermingseffectbeoordeling (GEB)

- De instelling voert een (tweejaarlijks terugkerende) evaluatie uit van de mogelijke effecten van de verschillende gegevensverwerking op de rechten en vrijheden van de betrokkenen. Deze evaluatie vindt eveneens plaats in geval van een wijziging in de verwerking van persoonsgegevens die specifiek de risico's wijzigt voor de privacy van de betrokken deelnemers en medewerkers.
- De instelling voert naar aanleiding van de evaluatie een volledige GEB uit in geval de verwerking van de persoonsgegevens:
  - in geval van een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
  - Bijzondere persoonsgegevens (ras, gezondheid) worden verwerkt;
  - Geautomatiseerde bewaking van publiek toegankelijke ruimtes.
- De beoordeling heeft betrekking op de gehele levenscyclus van persoonsgegevens van verzameling van verwerking tot verwijdering.
- In geval van herziening van of nieuwe verwerkingen van grote hoeveelheden persoonsgegevens, wordt vooraf bepaald wat de impact is van deze (gewijzigde) verwerking op de privacy van de deelnemers.
- Bij de GEB is altijd de FG betrokken.

In de toelichting hierbij staat dat informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, IT, 'facility management' en andere ondersteunende processen.

Indien uit een PIA blijkt dat de gegevensverwerking een hoog risico zou opleveren, dan moeten er maatregelen worden genomen om dat risico te mitigeren. Indien dat niet mogelijk is, is vanaf mei 2018 voorafgaand overleg met de AP noodzakelijk.

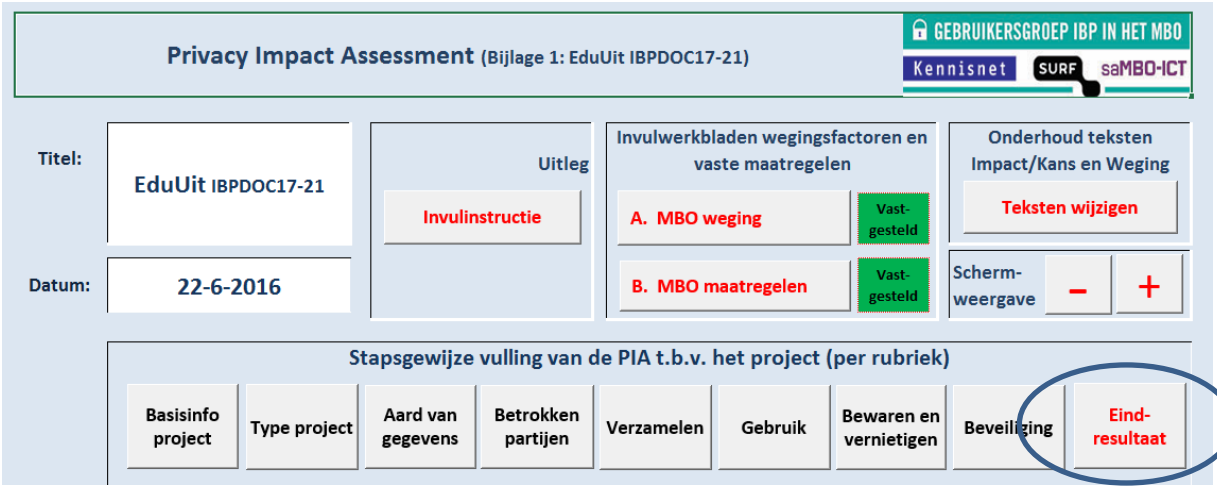
Een instelling moet dus vertrouwd raken met het uitvoeren van een PIA. Dit document laat voor een specifiek proces, namelijk dat van het gebruik van digitaal educatief leermateriaal (online leren) zien hoe je dat kunt aanpakken.

4.2 Bevindingen

Voor het uitvoeren van een PIA kun je een zelf een methode ontwikkelen maar je kan ook gebruik maken van een al ontwikkelde methodiek. Voor het mbo is gekozen om gebruik te maken van de PIA tool die ook door het hoger onderwijs wordt benut. Deze tool is vrij verkrijgbaar voor het mbo (saMBO-ICT site, groep ibp).

De uitgevoerde PIA voor het proces online leren is als losse Excel bijlage toegevoegd en te downloaden op de saMBO-ICT site. Zie: **Bijlage 1:** **PIA EduUit IBPDOC17**

Op grond van de AVG (privacy wetgeving) kan geconcludeerd worden dat er sprake is van de noodzaak om een PIA te maken. Dit kan je bijvoorbeeld doen als er sprake is van een nieuwe situatie, bijvoorbeeld aanbesteding van nieuwe materialen. Het kan ook zijn dat dit een keer tussendoor wordt georganiseerd. In ieder geval moet in mei 2018 sprake zijn van een op dit proces uitgevoerde PIA.
De volgende aanbevelingen komen naar voren op basis van de uitgevoerde PIA (zie het apart Excel sheet Bijlage 1 PIA EduUit).



1. Dataminimalisatie op basis van doelbinding.
2. Zorgen voor voldoende kwaliteit van data.
3. Beveiligen van data tegen lekken en hacken.
4. Authenticatie en autorisatie op basis van least privileges (minimale rechten).
5. Bewerkersovereenkomsten, juridisch normenkader.
6. Periodieke auditing.
7. Informeren van betrokkenen over gebruik van gegevens en recht op inzage/wijziging.
8. Mogelijk inregelen van opt-in/opt-out.
9. Zorgen voor klachtenprocedure.
10. Stel vooraf duidelijke bewaar termijnen vast en handel daarna.
11. Indien vernietigen niet mogelijk is beperk de toegang tot strikt noodzakelijke.

De uitkomst voor een specifiek digitaal educatief leermiddel xx kan zijn dat de leverancier een eigen(E) bewerkersovereenkomst heeft (BO) en dat die overeenkomst volgens het certificeringsschema (PB) van Kennisnet is goedgekeurd (G). Dat ziet er dan in het schema van de security architectuur als volgt uit:

Proces: **Online leren**	**29**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)* **Ja – E – G**

5. Bewerkersovereenkomst

Op grond van de PIA is een bewerkersovereenkomst met de leverancier van het betreffende digitaal educatief leermateriaal noodzakelijk. Hieronder een voorbeeld van hoe een volledige bewerkersovereenkomst van deze (fictieve) leverancier uit kan zien. De leverancier vult alleen de bijlagen (1 en 2) in en uiteraard punt 2 bij Partijen.

Bewerkersovereenkomst EduUit

Partijen:

1. Het bevoegd gezag van **<naam + rechtsvorm onderwijsinstelling>**, geregistreerd onder BRIN-nummer **<brin>** bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan **<adres>,** te **(<postcode>) <plaats>**, te dezen rechtsgeldig vertegenwoordigd door **<functie + naam>,** hierna te noemen: "**Onderwijsinstelling**".

   EN

2. De besloten vennootschap **EduUit B.V., gevestigd en kantoorhoudende aan Schoolstraatm1,** te **6461 RB Kerkrade**, te dezen rechtsgeldig vertegenwoordigd door **directeur Claessen** hierna te noemen: "**Bewerker**" .

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

Overwegen het volgende:

1. Onderwijsinstelling en Bewerker zijn een overeenkomst aangegaan waarbij <**concrete omschrijving van de door Bewerker in opdracht van Onderwijsinstelling te leveren producten/diensten**>, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Bewerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
2. Partijen wensen, mede gelet op het bepaalde in artikel 14 Wet bescherming persoonsgegevens, in deze Bewerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Bewerkersovereenkomst wordt verstaan onder:

1.1 Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;

1.2 Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;

1.3 Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;

1.4 Convenant: de meest recente versie van het *Convenant Digitale Onderwijsmiddelen en Privacy*, zoals gepubliceerd op www.privacyconvenant.nl;

1.5 Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, Wbp;

1.6 Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;

1.7 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;

1.8 School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerling volgsysteem (zoals bijvoorbeeld een LAS, LVS, SIS of KRS);
1.9 Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
1.10 Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
1.11 Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
1.12 Sub bewerker: de partij die door Bewerker wordt ingeschakeld als Bewerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst en de Product- en Dienstenovereenkomst;
1.13 Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1.1 Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
1.2 De Onderwijsinstelling verstrekt aan de Bewerker de opdracht tot Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst.

Artikel 3: Rolverdeling

3.1 Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verantwoordelijke. Bewerker is bewerker in de zin van de Wbp. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens.
3.2 Bewerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Bewerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Bewerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie moet de Onderwijsinstelling in staat stellen een keuze te maken met betrekking tot de aangeboden diensten als zodanig, en daarnaast een afzonderlijke keuze te maken voor eventueel aangeboden optionele diensten.
3.3 De in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, moeten in de Privacy Bijsluiter bij deze Bewerkersovereenkomst in begrijpelijke taal zijn beschreven, waarna de Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en).
3.4 De Onderwijsinstelling kan verplicht zijn de Verwerking van de Persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De Onderwijsinstelling onderzoekt of zij hiervan is vrijgesteld en doet melding bij de Autoriteit Persoonsgegevens indien zij hiertoe verplicht is.
3.5 Onderwijsinstelling en Bewerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de relevante privacywet- en regelgeving mogelijk te maken.

Artikel 4: Privacy convenant

4.1 Partijen onderschrijven de bepalingen in het Convenant Digitale Onderwijsmiddelen en Privacy.

Artikel 5: Gebruik Persoonsgegevens

5.1 Bewerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.
5.2 Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
5.3 De Bewerker dient in de Privacy Bijsluiter aan te geven of de Privacy Bijsluiter toeziet op een Leermiddel en Toets en/of School- en Leerlinginformatiemiddelen. Bewerker specificeert in de Privacy Bijsluiter voor welke (in het Convenant opgenomen) doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt. Indien aangegeven in de toelichting in de Privacy Bijsluiter, dient de Bewerker tevens aan te geven onder welke van de in het Convenant omschreven doeleinden bij het gebruik van het product en/of de dienst de Verwerking van Persoonsgegevens plaatsvindt.
5.4 Bewerker onthoudt zich van verstrekking van Persoonsgegeven aan een Derde, tenzij deze uitwisseling plaatsvindt in opdracht van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een op de Bewerker rustende

wettelijke verplichting. In geval van een wettelijke verplichting, verifieert Bewerker voorafgaande de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker. Daarnaast informeert Bewerker de Onderwijsinstelling – indien wettelijk toegestaan - onmiddellijk, zo mogelijk voorafgaand aan de verstrekking.

5.5 *SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN EEN ONDERWIJSKUNDIG RAPPORT, OVERSTAPDOSSIER OF DIGITAAL ONDERWIJS DOSSIER: In aanvulling op het bepaalde in lid 4, geldt dat indien Bewerker wordt verzocht Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde Derde, zijnde een andere onderwijsinstelling, de Bewerker slechts tot die verstrekking zal overgaan nadat deze onderwijsinstelling zijn administratieve onderwijsidentiteit (bijvoorbeeld BRIN of OiN), voor zover hij daarover beschikt, kenbaar heeft gemaakt.*

5.6 *SPECIFIEKE BEPALING IN GEVAL VAN DISTRIBUTIE VAN LEERMIDDELEN: Partijen zullen jaarlijks bij het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld, de Privacy Bijsluiter aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt, met betrekking tot de (digitale) leermiddelen die op de desbetreffende leermiddelenlijsten worden opgenomen.]*

Artikel 6: Geheimhouding

6.1 Bewerker zorgt er voor dat een ieder, waaronder haar werknemers, vertegenwoordigers en/of sub bewerkers, die betrokken zijn bij de Verwerking van de Persoonsgegevens deze gegevens als vertrouwelijk behandelt. Bewerker bewerkstelligt dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.

6.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Bewerker aan Onderwijsinstelling te verlenen diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 7: Beveiliging en controle

7.1 Bewerker zal, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Deze maatregelen zullen, met inachtneming van de stand van de techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.

7.2 De maatregelen zoals genoemd in artikel 7.1 omvatten in ieder geval:

a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkersovereenkomst worden verwerkt;
b. maatregelen om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;
c. maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling;
d. een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.

7.3 Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.

7.4 In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud en de frequentie van de rapportages die Bewerker aan de Onderwijsinstelling oplevert over de beveiligingsmaatregelen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Onderwijsinstelling moet treffen.

7.5 De Bewerker stelt de Onderwijsinstelling in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Bewerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, een geldige certificering of een gelijkwaardig controle- of bewijsmiddel.

7.6 In aanvulling op artikel 7, lid 4 heeft de Onderwijsinstelling te allen tijde het recht om, in overleg met de Bewerker en met inachtneming van een redelijke termijn, op eigen kosten, de door Bewerker genomen technische en organisatorische beveiligingsmaatregelen te laten toetsen door een onafhankelijke Register EDP auditor. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Bewerker in te schakelen gecertificeerde en onafhankelijke auditor die een derdenverklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

8.1 Bewerker heeft een passend beleid voor de omgang met Datalekken.

8.2 Indien Onderwijsinstelling dan wel Bewerker een Datalek vaststelt, dan zal deze de andere Partij onverwijld informeren. Bewerker verstrekt ingeval van een Datalek alle relevante informatie aan Verantwoordelijke met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Bewerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen. Aanvullend informeren Partijen elkaar onverwijld indien blijkt dat de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van Betrokken zoals bedoeld in artikel 34a, lid 2, Wbp.

8.3 Bewerker stelt bij een Datalek de Verantwoordelijke in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek Bewerker dient hierbij aansluiting te zoeken bij de bestaande processen die Verantwoordelijke 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 Wbp of andere regelgeving betreffende de Verwerking van de Persoonsgegevens, te voorkomen of te beperken.

8.4 In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. Partijen kunnen in onderling overleg bepalen of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten. Op verzoek van de Onderwijsinstelling kan Bewerker Onderwijsinstelling hierbij bijstaan en adviseren. De Onderwijsinstelling zal de Betrokkenen, indien wettelijk vereist, informeren over een dergelijke inbreuk. 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.

8.5 Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub b, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

9.1 Een klacht of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door de Bewerker onverwijld doorgestuurd naar de Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.

9.2 Bewerker verleent Onderwijsinstelling – voor zover redelijkerwijs mogelijk - volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Partijen zullen te goeder trouw overleggen over de redelijke verdeling van de eventuele kosten die hiermee gemoeid zijn.

Artikel 10: Verwerking buiten de Europese Economische Ruimte

10.1 Partijen zien er op toe dat voor zover Persoonsgegevens buiten de Europese Economische Ruimte (verder: EER) worden Verwerkt, dit alleen plaatsvindt conform wettelijke voorschriften, en eventuele verplichtingen die in dit verband op Onderwijsinstellingen rusten. Indien gegevens buiten de EER worden verwerkt wordt dit in Bijlage 1 aangegeven, inclusief een opgave van de landen waar de gegevens worden verwerkt.

Artikel 11: Inschakeling Subbewerker

11.1 Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.

11.2 Bewerker verplicht iedere Subbewerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na te leven met betrekking tot de Verwerking van Persoonsgegevens welke verplichtingen en maatregelen minimaal dienen te voldoen aan het bepaalde in deze Bewerkersovereenkomst.

11.3 Bewerker verplicht iedere Subbewerker contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

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

12.2 Onderwijsinstelling verplicht Bewerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Bewerkersovereenkomst 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.

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

12.4 Bewerker zal alle Subbewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkersovereenkomst en zal waarborgen dat alle Subbewerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Tegenstrijdigheid en wijziging Bewerkersovereenkomst

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

13.2 Indien Partijen van de artikelen in de Model Bewerkersovereenkomst 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 dan als Bijlage 3 aan deze Bewerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.

13.3 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, de doeleinden waaronder de Persoonsgegevens worden Verwerkt en het inschakelen van een (andere) Subbewerker. De wijzigingen zullen in Bijlage 1 worden opgenomen.

13.4 Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.

13.5 In het geval enige bepaling van deze Bewerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Bewerkersovereenkomst 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 14: Duur en beëindiging

14.1 Op deze Bewerkersovereenkomst is Nederlands recht van toepassing.

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

14.3 Deze Bewerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Bewerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Bewerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.

Bijlage 1 bij Bewerkersovereenkomst EduUit:

Privacy Bijsluiter, EduUit B.V.

EduUit 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.
EduUit 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 'verantwoordelijke' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt. EduUit is een 'bewerker', die uitvoering geeft aan de opdracht van een onderwijsinstelling.
De afspraken die hiervoor gelden, zijn vastgelegd in de Bewerkersovereenkomst van EduUit. 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 EduUit om gegevens te verwerken. Deze Privacy Bijsluiter stelt u tevens in staat om ouders en studenten te informeren over de verwerking van persoonsgegevens.

A. Algemene informatie

Naam product en/of dienst:	Deze Privacy Bijsluiter ziet op alle digitale leermiddelen die EduUit ontwikkelt voor het primair en voortgezet onderwijs. Een transparant overzicht van alle uitgangspunten rondom privacy is te vinden op www.EduUit.nl/privacy *(fictief)*.
Naam Bewerker en vestigingsgegevens:	EduUit B.V., Kerkrade.
Beknopte uitleg en werking product en dienst:	EduUit is een aanbieder van digitale leermiddelen. Binnen deze digitale leermiddelen worden persoonsgegevens verwerkt. Dit zijn bijvoorbeeld de gegevens die studenten 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 studenten 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.
Link naar uitgever en/of privacypagina:	www.EduUit.nl, www.EduUit.nl/privacy
Doelgroep:	PO, VO, MBO, HO,
Gebruikers:	De digitale leermiddelen zijn gericht op gebruik door studenten, studenten en docenten, leerkrachten en algemene gebruikers en organisaties en instellingen.

B. De specifieke diensten

EduUit 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 EduUit vinden primair plaats om met gebruikmaking van de digitale leermiddelen onderwijs te geven en studenten te kunnen volgen en begeleiden. Daaronder wordt verstaan:

Doelen van verwerking

- Identificatie

Voor unieke identificatie van de gebruiker van de producten en diensten van de educatieve oplossing van EduUit.

- Autorisatie

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

- Klassen en leerproces

Ter ondersteuning van het klasse- en leerproces; om bijvoorbeeld leerresultaten van studenten aan de leerkracht te kunnen terug koppelen in een resultaten dashboard voor alleen de leerkracht of aan een eventueel student administratiesysteem.

- Productontwikkeling en productverbetering

Voor productontwikkeling en productverbetering; hieronder valt ook statistisch onderzoek.

- 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.

- 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. Borgen van de continuïteit en goede werking van het digitale leermiddel.

- 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 EduUit en voor informatie over onderhoud en beheer van de applicatie.

Optionele verwerkingen

Tevens worden door EduUit 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 student administratiesystemen van de onderwijsinstelling.

C. Categorieën en soorten persoonsgegevens

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

Categorie van betrokkenen

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

Categorie van gegevens

- Identificatie
- Voornaam, tussenvoegsel, achternaam
- Emailadres
- Gebruiksgegevens en resultaten
- Klassen en leerproces
- Sociale laag: Persoonlijke en gedeelde notities
- Optimaliseren applicatie en content
- Mbo instellinginformatie BRIN

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 ons authenticatieplatform waarvoor een aparte registratie aanwezig is. Dit zorgt voor een ontkoppeling van het externe id van de mbo instelling met het interne id van EduUit.
Deze unieke identificatie maakt de overige categorieën en verzameldoelen mogelijk.

- Voornaam, tussenvoegsel, achternaam

Voor gepersonaliseerde toegang tot de aangeboden producten en diensten van EduUit. 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 EduUit gebruikt voor het verzenden van elektronische boodschappen over het product/de diensten van de educatieve applicatie en voor informatie over onderhoud en beheer van de diensten van EduUit.

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

- Mbo instellinginformatie BRIN

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 EduUit. Tevens voor interne controle, beveiliging van de diensten en fraudepreventie.

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's) zoals de Kennisnet federatie, Entree, Basispoort, Direct Access Framework Edu-iX/DAF (distributeurs) naar de uitgeverij. EduUit 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. Na het inloggen worden door EduUit 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 studenten met de lesstof heeft gedaan en wat het resultaat daarvan is.
Soorten van bijzondere persoonsgegevens:	In onze digitale leermiddelen worden in beginsel geen 'bijzondere persoonsgegevens' verwerkt in de zin van artikel 16 van de Wbp. 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 van onze systemen dan aan de publieke sites.

D. Algemene informatie over getroffen beveiligingsmaatregelen:

Voor de genomen veiligheidsmaatregelen verwijzen wij u naar Bijlage 2 van de Bewerkersovereenkomst.
Persoonsgegevens worden door EduUit verwerkt binnen Nederland. Een overzicht van de opslag en verwerking van subbewerkers die worden ingeschakeld door EduUit treft u hieronder.

E. Subbewerkers

Voor bepaalde verwerkingen van persoonsgegevens worden door EduUit sub bewerkers ingeschakeld.
U kunt hierbij denken aan:

- Ontwikkel- en hostingpartij en haar personeel als bewerker bij haar activiteiten rond applicatie- en technisch beheer van onderdelen van de educatieve applicaties.
- Personeel van EduUit en door EduUit gecontracteerde partijen die belast zijn met onderhoud en functioneel, applicatie en technisch beheer van de educatieve applicaties.

Als EduUit persoonsgegevens laat verwerken door een bewerker, zal EduUit er zorg voor dragen dat deze bewerker de gegevens uitsluitend voor de bovengenoemde doelen mag verwerken en voldoende waarborgen

biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen. EduUit zal met de bewerker een schriftelijke 'bewerkersovereenkomst' sluiten.

F. Regeling inzage- en correctierecht EduUit

De regeling inzage en correctierecht EduUit, zie www.EduUit.nl/privacy, geldt wanneer betrokkenen (studenten, docenten, gebruikers, ouders en andere wettelijke vertegenwoordigers) verzoeken om inzage in de persoonsgegevens die verwerkt worden door EduUit in haar rol als **Verantwoordelijke** conform de bepalingen in de Wet bescherming persoonsgegevens.
EduUit 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 '**verantwoordelijke**' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt.

Bovenstaande betekent dat studenten, ouders of wettelijke vertegenwoordigers die contact opnemen met uitgeverij EduUit 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 EduUit over uw kinderen heeft vastgelegd en kunt u dat verantwoorden.

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

Als u als mbo instelling in opdracht van een ouder of wettelijke vertegenwoordiger wilt dat EduUit stopt met verwerken van gegevens van een specifieke student, dan verzoeken wij u per e-mail contact opnemen met EduUit via privacy@EduUit.nl, met alle relevante informatie, inclusief een bewijs van inschrijving van de betreffende student op uw mbo instelling.
EduUit zal in uw opdracht de persoonsgegevens van het specifieke kind zo spoedig mogelijk proberen te verwijderen.

G. Contactgegevens

Voor vragen of opmerkingen over deze Privacy Bijsluiter of de werking van onze digitale leermiddelen, kunt u terecht bij: EduUit, t.a.v. Security Manager, Postbus 400, 6400 RB, Kerkrade. Onze helpdesk is telefonisch bereikbaar. Alle actuele contactinformatie vindt u op www.EduUit.nl/contact.

H. Versie

Deze Privacy Bijsluiter is voor het laatst bijgewerkt op 1 juli 2016.

Bijlage 2 bij Bewerkersovereenkomst EduUit:

Technische en organisatorische beveiligingsmaatregelen

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst
EduUit neemt passende technische en organisatorische maatregelen om de persoonsgegevens van uw studenten te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking

I. Maatregelen om persoonsgegevens te beschermen

Organisatie van informatiebeveiliging en communicatieprocessen

- EduUit heeft een informatie security management systeem (ISMS). Daarin is een informatiebeveiligingsbeleid vastgesteld, en organisatorisch een Security Manager aangewezen 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.
- Informatiebeveiliging is binnen EduUit 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.
- Alle medewerkers van EduUit hebben training gehad omtrent informatiebeveiliging.
- Jaarlijks wordt de scan van het College Bescherming Persoonsgegevens uitgevoerd, en 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 WBP en de richtsnoeren van het college bescherming persoonsgegeven, en de Europese Verordening Dataprotectie, en betrokkenheid bij de GEU rondom het Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen.

Personeel en leveranciers

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

Fysieke beveiliging en continuïteit van de middelen

- Er wordt zo veel mogelijk 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.

Rapportage

Bewerker rapporteert aan EduUit over updates of beveiligingsincidenten. De bewerker actualiseert de informatie en informeert contractpartijen en/of gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen.
De EduUit security officers rapporteren vervolgens aan de Security Manager, t.b.v. het ISMS overleg.
EduUit communiceert haar maatregelen rondom de technische en organisatorische maatrelen jaarlijks via de privacy bijsluiter. 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. bewerkersovereenkomst en privacy bijsluiter en zal de administratieve belasting voor de mbo instelling en de uitgeverij idealiter minimaal zijn.
Wet Meldplicht datalekken: EduUit heeft een Incident en Response Procedure ingericht waarbij er bij calamiteiten, waarbij er vastgesteld wordt dat er persoonsgegevens gelekt zijn, er binnen 72 uur contact zal worden gelegd met de verantwoordelijke instellingen. De verantwoordelijke instellingen zijn op dat moment verplicht om tevens binnen deze 72 uur na vaststelling van het incident een melding te doen bij de Autoriteit Persoonsgegevens (AP).
Updates rondom het privacystatement worden weergegeven op www.EduUit.nl/privacy.
In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van EduUit, www.EduUit.nl/contact.

Versie

Deze bijlage is voor het laatst bijgewerkt op 1 juli 2016.
Deze bijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen -, een initiatief van de MBO-Raad, de verschillende betrokken ketenpartijen (GEU, KBb-e en vDOD), het ministerie van Onderwijs, Cultuur en Wetenschappen en het ministerie van Economische Zaken

Bijlage 1: Framework Informatiebeveiliging en privacy in het mbo