

Bijlage 1: Privacy Bijsluiter

Behorende bij verwerkersovereenkomst de Digitale Leermiddelen, van Schoolsupport Uitgeverij BV

Versie: 01-03-2023

Schoolsupport Uitgeverij BV is een educatieve uitgeverij die digitale onderwijsmiddelen aanbiedt voor gebruik in het onderwijs waarbij persoonsgegevens worden verwerkt. Wij vinden het belangrijk om uiterst zorgvuldig met deze persoonsgegevens om te gaan. Wij stellen daarom hoge eisen aan de betrouwbaarheid en veiligheid van onze systemen. Leerresultaten en de gegevens van onze gebruikers beschouwen wij te allen tijde als privacygevoelige gegevens.

Schoolsupport Uitgeverij BV heeft het 'Convenant Digitale Onderwijsmiddelen en Privacy' onderschreven. 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. Schoolsupport Uitgeverij BV is een 'verwerker', die uitvoering geeft aan de opdracht van een onderwijsinstelling.

De afspraken die hiervoor gelden, zijn vastgelegd in de Verwerkersovereenkomst van Schoolsupport Uitgeverij BV. De bijlagen vormt een onlosmakelijk onderdeel van de Verwerkersovereenkomst. In bijlage 1 staat beschreven welke opdracht u, als Onderwijsinstelling, Schoolsupport Uitgeverij BV geeft ten aanzien van de verwerking van persoonsgegevens in de Digitale Leermiddelen. Deze bijlage stelt u tevens in staat om ouders en leerlingen hierover te informeren.

1. Algemene informatie

Naam product en/of dienst

Deze bijlage heeft betrekking op de Digitale Leermiddelen van Schoolsupport Uitgeverij BV.

Naam Verwerker en vestigingsgegevens

Schoolsupport Uitgeverij BV te Leerlooierstraat 6, (4871 EN) Etten-Leur.

Beknopte uitleg en werking product en dienst

In de groep Digitale Leermiddelen vallen de volgende producten en diensten:

- Bareka Online Rekentoetsen
- Licentiebeheersysteem (hierna te noemen: 'LBS'), Identityprovider (hierna te noemen: 'idp')
- Schoolsupport Leesplatform (DC Online, Get Started, Kits/Klap, NT2, Read Along, Snappie, TekstVaardig, Themaplein, Wereldbieb)
- Schoolsupport Rekenplatform (Rekensprint Online, ATR)
- Schoolsupport Dashboard

De verwerking van persoonsgegevens binnen deze producten en diensten heeft betrekking op:

- Het toegang krijgen tot producten door middel van een inlogprocedure;
- Het aanmaken en beheren van groepen en leerlingen – en het aanmaken en beheren van taken of leeslijsten voor leerlingen, al dan niet per leerling;
- Het publiceren van opdrachten door leerlingen.

Op basis van de resultaten van het gebruik van de Digitale Leermiddelen kan de onderwijsinstelling zelf conclusies trekken over de leerontwikkeling van leerlingen.

Link naar uitgever en/of productpagina

www.schoolsupport.nl; app.schoolsupport.nl; www.toegangonderwijs.nl

Doelgroep

Primair onderwijs; Praktijkhouders; VO (VSO, PrO), MBO

Gebruikers

De Digitale Leermiddelen richten zich op gebruik door: directie, hoogbegaafdheidsspecialisten, ICT-coördinatoren, intern begeleiders, taal-, lees- en rekencoördinatoren, leerkrachten en leerlingen.

2. Doeleinden voor het verwerken van persoonsgegevens

De Digitale Leermiddelen kennen een onderscheid tussen verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst, en optionele verwerkingen.

Verwerkingen die een onlosmakelijk onderdeel vormen van de Digitale Leermiddelen

De verwerkingen door Schoolsupport Uitgeverij BV vinden primair plaats om onderwijsinstellingen in staat te stellen om met gebruikmaking van de digitale leermiddelen onderwijs te geven en leerlingen te kunnen volgen en begeleiden.

Bij het gebruik van De Digitale Leermiddelen vinden altijd de volgende verwerkingen plaats, in lijn met artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy:

- de opslag, analyse en interpretatie van leer- en testresultaten;
- het terugontvangen door de onderwijsinstelling van leer- en testresultaten;
- het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
- het verkrijgen van toegang tot de aangeboden digitale leermiddelen, waaronder de identificatie, authenticatie en autorisatie;
- de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik, en het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte persoonsgegevens;
- de continuïteit en goede werking van het digitale leermiddel, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
- het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.

Optionele verwerkingen bij de Digitale Leermiddelen

Bij het gebruik van de Digitale Leermiddelen kunnen met specifieke toestemming van de onderwijsinstelling ook andere verwerkingen plaatsvinden. Onderwijsinstellingen hebben voor deze verwerkingen een actieve keuzeoptie en gaan in de Digitale Leermiddelen of anderszins expliciet akkoord met de verwerkingen voordat deze plaatsvinden. Het betreft de volgende verwerkingen:

- het kunnen uitwisselen van leer- en testresultaten met dashboards die de onderwijsinstelling in gebruik heeft;
- het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale onderwijsmiddelen;

- het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.

3. Categorieën en soorten persoonsgegevens

Bij het gebruik van de Digitale Leermiddelen worden de volgende persoonsgegevens verwerkt.

Verwerkte persoonsgegevens voor autorisatie en authenticatie

Het verkrijgen van toegang tot digitale leermiddelen verloopt via Stichting Basispoort. Hierdoor kan via één inlogprocedure toegang worden verkregen tot digitale leermiddelen van verschillende uitgeverijen.

Schoolsupport Uitgeverij BV ontvangt van Basispoort voor iedere leerling:

- Basispoort ID;
- LAS key en/of indien beschikbaar het ECK-ID;
- naam;
- jaargroep;
- klas;

Schoolsupport Uitgeverij BV ontvangt van Basispoort voor iedere leerkracht:

- Basispoort ID;
- LAS key;
- naam;
- klas;
- e-mailadres;
- optioneel: rol (ICT-coördinator, RT'er, IB'er of Stagiair).

De kern van de dienstverlening van Basispoort is dat in opdracht van de onderwijsinstelling aan leerkrachten en leerlingen toegang wordt verleend tot het digitale onderwijsmiddel van één uniforme inlogprocedure. Stichting Basispoort ontvangt geen leerresultaten van uitgevers.

Verwerkte persoonsgegevens voor autorisatie en authenticatie zonder Basispoort:

Het verkrijgen van toegang tot digitale leermiddelen verloopt via toegangonderwijs.nl en het daarmee gekoppelde LBS, dat de autorisatie en authenticatie van gebruikers doet en licentietoegangen vrijgeeft. Schoolsupport Uitgeverij BV ontvangt van LBS voor iedere leerling:

- een uniek ID;
- naam;
- jaargroep;
- klas;

Schoolsupport Uitgeverij BV ontvangt van LBS voor iedere leerkracht:

- een uniek ID;
- naam;
- klas;
- e-mailadres;

Verwerkte persoonsgegevens bij gebruik van het leermiddel

Na het inloggen worden door Schoolsupport Uitgeverij BV vervolgens de gegevens verwerkt die gebruikers invullen bij:

- oefenopgaven;
- toetsopgaven;
- inlogactiviteit gebruikers en wijziging van (persoons)gegevens.

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.

Optionele persoonsgegevens

Niet van toepassing

Soorten van gegevens

In de Digitale Leermiddelen worden geen bijzondere categorieën van persoonsgegevens verwerkt in de zin van artikel 9 van de AVG.

4. Bewaartermijnen

De verkregen persoonsgegevens in de Digitale Leermiddelen worden na verloop van tijd gewist. In de tabel hieronder staan de bewaartermijnen.

Persoonsgegevens	2 jaar na de laatst geregistreerde activiteit
Loggen van inlogactiviteit gebruikers en wijziging van (persoons)gegevens	De logging van activiteiten en wijzigingen van gegevens blijft voor 13 maanden bewaard, conform de beveiligingseisen certificeringsschema. En zal hierna binnen 1 maand automatisch worden verwijderd.

Subverwerkers en locatie van opslag en verwerking van persoonsgegevens

Voor de verwerking van persoonsgegevens worden door Schoolsupport Uitgeverij BV de volgende subverwerkers ingeschakeld.

Naam:	Omschrijving:	Land van opslag en verwerking:
AWS	ECS; RDS database (Rekensprint)	Ierland
Basispoort, Ochten	Single-sign-on toegangsdienst	Nederland
Dsens IT, Amsterdam	IT-development	Nederland
Harm Bandstra	IT-development Bareka	Nederland
Hetzner	Hostingprovider	Duitsland

MailCamp, Amsterdam	ESP	Nederland
Microsoft	Azure ; E-mailprovider	Nederland
NLWare, Amsterdam	IT-development	Nederland
Readiant BV, Groningen	Applicatiebeheerder	Nederland
TransIP, Groningen	Hostingprovider	Nederland
MultiSafe pay, Amsterdam	Payment provider	Nederland
Socho IT, Huizen	ERP	Nederland
Usersnap	Customer feedback	Oostenrijk

5. Contactgegevens

Voor vragen of opmerkingen over deze bijlage of de werking van onze digitale onderwijsmiddelen, kunt u terecht bij:

Schoolsupport Uitgeverij BV helpdesk: service@schoolsupport.nl

Onze helpdesk is telefonisch bereikbaar via (+31) (0)76-2050101.

Of raadpleeg onze contactpagina op: www.schoolsupport.nl/nl/contact

Indien er voor ons reden is om contact op te nemen, doen wij dat in beginsel per email met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4.

Paraaf



Onderwijsinstelling

Verwerker

Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.

Bijlage 2: Beveiligingsbijlage

Behorende bij verwerkersovereenkomst de Digitale Leermiddelen, van Schoolsupport Uitgeverij BV

Versie: 01-03-2023

Schoolsupport Uitgeverij BV heeft, overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst passende technische en organisatorische maatregelen genomen om de verwerking van persoonsgegevens aantoonbaar te beveiligen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

1. Maatregelen die Schoolsupport Uitgeverij BV heeft genomen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
- Een systeem van autorisatie waardoor enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie;
- Er is een coördinator informatiebeveiliging die de risico's omtrent de verwerking van persoonsgegevens inventariseert, het beveiligingsbewustzijn stimuleert, voorzieningen controleert en maatregelen treft die zien op naleving van het informatiebeveiligingsbeleid. Deze coördinator is bereikbaar op het volgende emailadres: privacy@schoolsupport.nl
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid;
- Er is een proces ingericht voor communicatie over informatiebeveiligingsincidenten;
- Met medewerkers worden geheimhoudingsverklaringen afgesloten en worden informatiebeveiligingsafspraken gemaakt;
- Het bewustzijn, opleiding en training ten aanzien van informatiebeveiliging wordt gestimuleerd.

2. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden, zoals beschreven in het Certificeringsschema informatiebeveiliging en privacy ROSA. Zie: https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/.

Toetsvorm	Self assessment, uitgevoerd op 01-02-2023 op basis van toetsingskader 3.0		
Uitvoerder toets	Dhr. M. van Diepen (in samenspraak met afdeling development Schoolsupport), Technisch projectleider (Schoolsupport), Schoolsupport Uitgeverij BV		
Inlogpagina	app.schoolsupport.nl		
BIV-classificatie	Beschikbaarheid = M Integriteit = M Vertrouwelijkheid = M		
Categorie	Maatregelen	Compliance	Uitleg
Beschikbaarheid	Ontwerp	alternatieve maatregel	De meest cruciale onderdelen zijn redundant uitgevoerd door Schoolsupport of door de leverancier van de betreffende infrastructuur. Een complete redundante infrastructuur is niet kosteneffectief realiseerbaar.
	Capaciteit beheer	alternatieve maatregel	Er wordt gezorgd voor voldoende overcapaciteit, zodat ook onverwachte groei kan worden opgevangen. Systemen worden dynamisch geschaald, zodanig dat tijdens piekuren (aanvang schooltijd, na de lunch) de capaciteit van de server zich aanpast aan de hoeveelheid gebruikers die zich aandienen. Monitoring van het gebruikersverkeer vindt plaats om op basis daarvan de capaciteit aan te passen, zodat er voldoende overcapaciteit beschikbaar blijft.
	Onderhoud	voldaan	Voor de recent ontwikkelde systemen wordt onderhoud uitgevoerd zoals hier voorgeschreven. Afdeling development houdt via een gedeeld patch en dependency-management document de actualiteit van de software actief in de gaten. Legacy systemen waarop dit niet van toepassing was, zijn inmiddels uitgefaseerd.

	Testen	alternatieve maatregel	<p>Na een release wordt er een regressietest gedaan waarmee de basisfunctionaliteit wordt doorlopen.</p> <p>Verder wordt er voor voldoende overcapaciteit gezorgd om de performance te kunnen garanderen.</p> <p>Systemen worden aan stresstesten onderworpen wanneer de core van applicaties naar productie worden gebracht.</p> <p>Alvorens applicaties (m.n. Rekensprint) naar productie gaan worden ze eerst uitvoerig getest in een bèta-omgeving.</p> <p>Bij een loadtest is het lastig om realistisch gebruikersverkeer te realiseren. Daarom worden specifieke performance bottlenecks uitvoerig gemonitord m.b.v. gespecialiseerde software.</p>
	Monitoring	voldaan	
	Herstel	voldaan	<p>In het kader van Cloudhosting wordt voldaan aan de gestelde eisen.</p> <p>Voor de platformen waar gebruik wordt gemaakt van virtuele machines is uit kosten overwegingen gekozen voor "cold stand-by"</p> <p>Legacy systemen zijn per februari 2023 uitgefaseerd, vervangende systemen voldoen aan gestelde eisen.</p>
Integriteit	Herleidbaarheid (gebruikers)	voldaan	
	Backup	voldaan	<p>Dagelijks worden er back-ups gemaakt en periodiek gecontroleerd op integriteit.</p> <p>Per maart 2023 worden back-ups tevens verstuurd naar een storage machine.</p>
	Application controls	voldaan	
	Onweerlegbaarheid	voldaan	
	Herleidbaarheid (technisch beheer)	voldaan	<p>Afdeling development werkt met een change/release kalender waarop changes/hotfixes/deloys per applicatie en serverconfiguraties bijgehouden worden.</p>

	Controle integriteit	voldaan	Afdeling development houdt via een gedeeld patchmanagement- en dependency document de actualiteit van de software actief in de gaten. Legacy systemen waarop dit niet van toepassing is, zijn uitgefaseerd per februari 2023.
	Onweerlegbaarheid (toepassing)	voldaan	De door Schoolsupport gebruikte clouddiensten ondersteunen default vereisten t.a.v. logging technisch beheer. Dit geldt ook voor de systemen die dedicated gehost worden.
Vertrouwelijkheid	Levenscyclus gegevens	alternatieve maatregel	Persoonsgegevens worden conform de wettelijke regels, centraal en encrypted opgeslagen. Persoonsgegevens worden uiterlijk 2 jaar na de laatst geregistreeerde activiteit automatisch verwijderd uit onze systemen. Data opgebouwd bij het werken met educatieve applicaties wordt geanonimiseerd (niet herleidbaar) opgeslagen in de databases van de educatieve applicaties. Geanonimiseerde data (voortgang behaald bij het werken met de educatieve applicaties) kan voor analyse en productverbetering worden gebruikt.
	Logische toegang	alternatieve maatregel	Afdeling IT van Schoolsupport ziet erop toe dat accounts persoonlijk identificeerbaar zijn, en passen bij de rol van een medewerker. Daarnaast passen we waar mogelijk 2FA toe.
	Fysieke toegang	voldaan	
	Netwerk toegang	voldaan	Cloudoplossing dwingen default de minimale maatregelen af. Overige genoemde zaken zijn niet van toepassing voor onze situatie.
	Scheiding omgevingen	voldaan	We beschikken over een OTP omgeving voor alle platformen die voldoen aan genoemde vereisten.
	Transport en fysieke opslag	alternatieve maatregel	Opslag die persoonsgegevens bevat, is van encryptie voorzien.

			De opslag van persoonsgegevens is centraal geregeld, aan de kant van educatieve applicaties werken we met geanonimiseerde data.
	Logging	voldaan	
	Omgaan met kwetsbaarheden	voldaan	

3. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Schoolsupport Uitgeverij BV heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zullen wij de verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk, samenvatting van de inbreuk waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (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 de inbreuk;
- Hoe de inbreuk is ontdekt;
- De maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- Of de bij de inbreuk betrokken gegevens versleuteld, gehasht etc. waren;
- Benoemen van groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep Betrokkenen;
- Wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor betrokkene(n);
- De hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere gegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van) beveiligingsincident en/of Datalek zal onze coördinator informatiebeveiliging, in beginsel per email contact opnemen met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4. De coördinator informatiebeveiliging is tevens aanspreekpunt voor het geval de Onderwijsinstelling contact wil opnemen over een beveiligingsincident en/of Datalek. De coördinator informatiebeveiliging is bereikbaar op het volgende mailadres: privacy@schoolsupport.nl.

Paraaf



Onderwijsinstelling

Verwerker

Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.

Overzicht van scholen die vallen onder het bevoegd gezag van het bestuur

Naam schoolbestuur	
Adres schoolbestuur	
Administratienummer schoolbestuur ^{*)}	
De contactpersoon namens het schoolbestuur ^{**)}	
Mailadres van de contactpersoon	

^{*)} BRIN-, RIO of KVK-nummer.

^{**)} Bedoeld wordt degene die bevoegd/gemandateerd is om namens de Onderwijsinstelling opdrachten en instructies aan de Verwerker te verstrekken en die in het geval van een datalek door de Verwerker wordt geïnformeerd.

Overzicht van scholen

BRIN -6	schoolnaam	plaats	e-mail adres

Indien dit overzicht geactualiseerd moet worden, zal het schoolbestuur de wijzigingen door geven aan de verwerker.

Paraaf

Onderwijsinstelling

Verwerker

Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBb-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.