Bijlage 1

Privacy Bijsluiter (digitale) leermiddelen en educatieve diensten voor het voortgezet onderwijs van Blink

Blink is een educatieve uitgeverij die verschillende (digitale) producten en diensten (**'leermiddelen'**) aanbiedt voor gebruik in het onderwijs waarbij persoonsgegevens worden verwerkt. Wij vinden het belangrijk om uiterst zorgvuldig met deze persoonsgegevens om te gaan.

Blink heeft het Privacyreglement van haar brancheorganisatie GEU en het 'Convenant Digitale Onderwijsmiddelen en Privacy -Leermiddelen en Toetsen' 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. Blink is een verwerker, die uitvoering geeft aan de opdracht van een onderwijsinstelling.

De afspraken die hiervoor gelden, zijn vastgelegd in de Verwerkersovereenkomst van Blink. Deze Privacy Bijsluiter vormt een onlosmakelijk onderdeel van de Verwerkersovereenkomst.In deze 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 Blink om gegevens te verwerken. Deze Privacy Bijsluiter stelt u tevens in staat om ouders en leerlingen te informeren over de verwerking van persoonsgegevens.

A. Algemene informatie

Naam product en/of dienst:
Digitale Leermiddelen VO van Blink via docent- en leerlingomgevingen van verderop genoemde lesmethodes.

Naam Verwerker en vestigingsgegevens:
Blink, Den Bosch. Blink is een aanbieder van (digitale) leermiddelen en educatieve diensten.

Beknopte uitleg en werking product en dienst:
In de leermiddelen voor VO vallen de volgende producten en diensten:

- Blink Nederlands | Plot26 – Methode Nederlands
- Blink Nederlands bovenbouw – Methode Nederlands
- Blink Geschiedenis | Saga – Methode geschiedenis
- Blink Engels VO | Wired – Methode Engels

Binnen deze producten en diensten worden de volgende persoonsgegevens verwerkt:

- Om toegang te krijgen tot de Digitale Leermiddelen moeten gebruikers inloggen. Daarbij worden ook persoonsgegevens verwerkt.
- De Digitale Leermiddelen bevatten oefenmateriaal, waaronder oefenopgaven en toetsen. De gegevens die leerlingen invullen bij het gebruik van het leermiddel, zoals in een oefenopgaaf of toets worden verwerkt door Blink.
- Het platform achter de digitale leermiddelen koppelt resultaten van het gebruik door leerlingen terug aan een leerkracht. 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 productpagina:

- www.blink.nl
- www.blink.nl/blink-nederlands-onderbouw
- www.blink.nl/blink-nederlands-bovenbouw
- www.blink.nl/blink-geschiedenis
- www.blink.nl/blink-engels-vo

Doelgroep:
Voortgezet onderwijs, alle leerjaren, alle niveaus.

Gebruikers:
De digitale leermiddelen zijn gericht op gebruik door leerlingen, leraar, ict-coördinator.

B. Doeleinden voor het verwerken van gegevens en specifieke diensten

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

Verwerkingen die een onlosmakelijk onderdeel vormen van Digitale Leermiddelen van Blink

De verwerkingen door Blink vinden primair plaats om onderwijstellingen 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 van Blink vinden altijd de volgende verwerkingen plaats:

- De opslag van leer-en testresultaten; bijvoorbeeld gemaakte opdrachten en toetsen in de digitale leeromgeving;
- Het terugontvangen door de onderwijsinstelling van leer-en testresultaten;
- Om adaptief leermateriaal en gepersonaliseerde leerwegen (‘adaptiviteit’) mogelijk te maken, waaronder de mogelijkheid voor leerlingen om op hun eigen tempo te werken. Dit gebeurt door de beoordeling van leer-en testresultaten om leerstof en testmateriaal te verkrijgen, dat is afgestemd op de specifieke leerbehoefte van een leerling;
- De beoordeling van de leer-en testresultaten van één leerling ten opzichte van de resultaten van een normgroep, om inzicht te krijgen hoe een leerling presteert ten opzichte van deze groep;
- Het geleverd krijgen/in gebruik kunnen nemen van de digitale leermiddelen;
- Het verkrijgen van toegang tot de aangeboden digitale leermiddelen, waaronder de identificatie, authenticatie en autorisatie; bijvoorbeeld het invoeren van inloggegevens zoals gebruikersnaam, e-mailadres en een wachtwoord.
- 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 na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
- Het verwerken van gegevens tot volledig geanonimiseerde data om daarmee de kwaliteit van het onderwijs te verbeteren;
- Het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale leermiddelen.

Optionele verwerkingen

Bij het gebruik van de Digitale Leermiddelen van Blink kunnen met specifieke toestemming van de onderwijsinstelling ook andere verwerkingen plaatsvinden. Onderwijsinstellingen hebben voor deze verwerkingen een actieve keuze optie en gaan in het digitale leermiddel expliciet akkoord met de verwerkingen voordat deze plaatsvinden.Het betreft verwerkingen in het kader van:

- Het bewaren van leer-en testresultaten; denk hierbij aan de opslag van gegevens van leerlingen over de jaren heen. (Deze verwerking wordt op datum van publicatie nog niet door Blink aangeboden);
- Extern onderzoek en analyse op basis van strikte voorwaarden zoals vastgesteld binnen het Ketenplatform van het ‘Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen’. (Deze verwerking heeft nog niet plaatsgevonden en staat op datum van publicatie van dit document ook niet gepland);
- De beoordeling van leer-en testresultaten om leerstof en testmateriaal te verkrijgen, dat is afgestemd op de specifieke leerbehoefte van een leerling. (Dit gaat om verzoeken van individuele scholen).

C. Categorieën en soorten persoonsgegevens

Bij het gebruik van Digitale leermiddelen van Blink worden alleen identificerende persoonsgegevens verwerkt.

Omschrijving van de verwerkte persoonsgegevens:
Het verkrijgen van toegang tot digitale leermiddelen verloopt via het platform van Blink middels een koppeling met Directe Toegang (directetoegang.nl). Hierdoor kan via één inlogprocedure toegang worden verkregen tot digitale leermiddelen van verschillende methodes. Alternatief voor het inloggen via Directe Toegang is het inloggen via de Entree Federatie van Kennisnet waarlangs dezelfde gegevens worden verwerkt als via Directe Toegang. Mocht een school niet met Directe Toegang of de Entree Federatie gekoppeld zijn is het mogelijk om direct op de methodewebsite van Blink in te loggen.

De kern van de dienstverlening van het platform van Blink is dat in opdracht van de school aan docenten en leerlingen toegang wordt verleend tot online educatief materiaal door middel van één uniforme inlogprocedure.

Blink ontvangt van via Directe Toegang voor iedere leerlingen docent:

- Uniek ID van de gebruiker (uid);
- ECK-iD;
- Naam (voornaam, tussenvoegsel, achternaam);
- Uniek ID van de school;
- Naam van de school.

Docenten kunnen daarnaast ook inloggen met een e-mailadres/wachtwoord-combinatie.

Met uitzondering van de achternaam is deze set conform de standaard attributenset van Edu-K. De achternaam wordt opgeslagen voor het gebruik in de klas bij de herkenning van leerlingen in Blink Studio. Het gebruik van planning-en resultaten schermen wordt hierdoor vereenvoudigd voor de leerkracht.

De kern van de dienstverlening van Directe Toegang is dat in opdracht van de onderwijsinstelling aan docenten en leerlingen toegang wordt verleend tot online educatief materiaal door middel van één uniforme inlogprocedure. Directe Toegang ontvangt geen leerresultaten van uitgevers en wisselt deze evenmin uit.

Verwerkte persoonsgegevens bij gebruik van het leermiddel:
Na het inloggen worden door Blink vervolgens de gegevens verwerkt die gebruikers invullen bij het gebruik van het leermiddel, zoals in een oefenopgave 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.

Optionele persoonsgegevens:
Niet van toepassing.

Soorten van gegevens:
In de Digitale Leermiddelen van Blink worden geen ‘bijzondere persoonsgegevens’ verwerkt in de zin van artikel 16 van de Wbp. Op basis van de resultaten van het gebruik van de Digitale Leermiddelen kan de onderwijsinstelling zelf conclusies trekken over eventuele beperkingen in de leerontwikkeling en de oorzaak daarvan. Leerresultaten en de gegevens van onze gebruikers beschouwen wij te allen tijde als privacygevoelige gegevens, waarbij wij hoge eisen stellen aan de betrouwbaarheid en veiligheid van onze systemen.

Bewaartermijn:
Blink verwijdert de verkregen persoonsgegevens in Digitale Leermiddelen VO van Blink na verloop van tijd. In de tabel hieronder staan de bewaartermijnen.

Uniek ID van de gebruiker	1 jaar na afmelding
ECK-iD	Maximaal 6 jaar na aanmelding mits leerling nog in het VO zit en met de lesmethode wordt gewerkt. De reden hiervoor is de mogelijkheid tot het kunnen opbouwen van een leerlingportfolio.
Naam	1 jaar na afmelding
Leerlingresultaten	Maximaal 6 jaar na aanmelding mits leerling nog in het VO zit en met de lesmethode wordt gewerkt. De reden hiervoor is de mogelijkheid tot het kunnen opbouwen van een leerlingportfolio.

D. Algemene informatie over getroffen beveiligingsmaatregelen:

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

Persoonsgegevens worden door Blink verwerkt binnen Europa. Een overzicht van de plaats van opslagen verwerkingen door subverwerkers die worden ingeschakeld door Blink treft u hieronder.

E. Subverwerkers

Voor de ontwikkeling van (delen van) de verschillende toepassingen worden door Blink subverwerkers ingeschakeld. Hierbij worden persoonsgegevens verwerkt.

Naam	Omschrijving	Land van opslag en verwerking	Producten
Google	Hostingpartij van het educatieve platform waarop de lesomgeving van Blink is gebaseerd.	België	- Blink Nederlands - Blink Geschiedenis - Blink Engels
Webmine	Ontwikkelaar creatieve websites en apps.	Nederland	- Werkwoordspelling app van PLOT26

F. Contactgegevens

Voor vragen of opmerkingen over deze Privacy Bijsluiter of de werking van onze digitale leermiddelen, kunt u terecht bij: Blink, Koningsweg 66 Den Bosch.

Onze helpdesk is telefonisch bereikbaar via 073 – 85 000 22 of via privacy@blink.nl.
Meer informatie treft u op https://www.blink.nl en https://www.blink.nl/privacy.

G. Versiebeheer

Versie	Datum	Wijzigingen
1.0	25-05-2018	AVG van toepassing, introductie privacybijsluiter volgens Privacy Convenant
2.0	14-07-2020	Update bijlage 2, self-assessment.

2.1	23-09-2021	Spelling check; Uitbreiding VO-methoden;
3.0	30-11-2021	Aanpassingen bijlage 2, self-assessment. Er is een nieuwe, kritischer manier van self-assessment gehanteerd waardoor een aantal onderdelen van ‘Voldaan’ naar ‘Niet voldaan’ is gegaan. Tevens is een volgorde van verwerking van deze punten toegevoegd.
3.1	20-01-2022	Opschoning document, herformulering uitleg bij maatregelen.

Bijlage 2

Beveiliging bijlage

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst.

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Blink hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Medewerkers en gegevens	Handelingen
Medewerkers van de klantenservice hebben toegang tot licentie informatie. Zij kunnen onder meer zien voor welke leerlingen een digitaal leermiddel is geactiveerd. De klantenservice heeft geen inzage in leerresultaten van leerlingen.	Administratieve handelingen in het kader van de werking van leermiddelen en licenties. Ondersteuning van de eindgebruiker.
Ontwikkelaars en specialisten hebben toegang tot sets van resultaten van gebruik van leermiddelen en 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-database beheerders hebben toegang tot de databases.	De handelingen van IT-database beheerders zijn gericht op continuïteit en optimalisatie van de systemen van Blink.

II. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking.

Organisatie van informatiebeveiliging en communicatieprocessen

- Blink beschikt over een actief informatiebeveiligingsbeleid.
- Blink heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.

- Blink heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiliging afspraken gemaakt.
- Medewerkers hebben op grond van een autorisatie systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
- De geheimhouding van privacygevoelige persoonsgegevens en informatiebeveiliging wordt opgenomen in het huishoudelijke regelement van Blink.

Beveiliging en continuïteit van de middelen, het netwerk, de server en de applicatie
Blink heeft het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/) gebruikt als toetsingskader en voor het creëren van een solide basis niveau van informatiebeveiliging en privacy voor [naam product(groep)]. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Toetsvorm	Self-assessment		
Uitvoerder toets	Blink, Thomas van der Slot		
BIV-classificatie	Beschikbaarheid = 3; Integriteit = 2; Vertrouwelijkheid = 2		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Niet voldaan	We hebben een RTO van maximaal 8 uur, maar geen recovery test 4x per jaar.
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Niet voldaan	Er worden nog geen gebruikssimulaties of pro-actieve performancetesten ingezet.
	Software	Niet voldaan	Urgente security patches worden wel uitgevoerd, maar niet dmv. een geautomatiseerde controle. Er

			is hiervoor wel al een tool in ontwikkeling.
	Actuele dreigingen	Niet voldaan	Actieve bescherming tegen dreigingen is nog niet over de gehele linie ingezet.
Integriteit	Herleidbaarheid (gebruikers)	Niet voldaan	Er is reeds veel herleidbaar, het ontbreekt op dit punt nog op de herleidbaarheid welke exacte gegevens gewijzigd zijn. Dit is nu op objectniveau beschikbaar (inclusief datum van wijziging), maar nog niet op attribuutniveau.
	Backup	Niet voldaan	Restore tests worden nog niet op reguliere basis uitgevoerd.
	Application controls	Niet voldaan	Controle wordt vnl. via syntax-controle gedaan; Data-wijzigingen worden niet consequent gelogd, en logging wordt niet gecontroleerd.
	Onweerlegbaar-heid (van gegevens)	Niet voldaan	Wijziging van persoonsgegevens wordt niet gelogd. Zie ook *Integriteit - Herleidbaarheid.* Daarnaast wordt de logging nog niet gecontroleerd op afwijkende patronen. Ontwikkelingen zijn hiervoor gaande.
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Niet voldaan	Er is nog geen structurele controle voor de integriteit van de software.
	Actuele dreigingen (ransomware)	Niet voldaan	Een rollback naar een gecontroleerde situatie van 24 uur geleden is mogelijk. Er is nog geen goede aanvalsdetectie.
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Niet voldaan	Er is nog geen periodieke controle van actieve accounts versus actieve medewerkers.
	Fysieke toegang	Voldaan	

	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Niet voldaan	Toegang tot de productieomgeving wordt nog niet periodiek gecontroleerd.
	Transport en fysieke opslag	Niet voldaan	Er is nog geen encryptie voor extern verkeer.
	Logging	Niet voldaan	Er is nog geen loggingsysteem voor de toegang tot de toepassingen. Schooljaar 2021-2022 is een begin gemaakt met een loggingsysteem.
	Toetsing	Voldaan	
	Actuele dreigingen (hack)	Niet voldaan	Er is nog geen tool om hacks te kunnen detecteren en om ertegen te beschermen.

III Omschrijving van de 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.

De systemen van Blink worden (periodiek) gecontroleerd op veiligheid door bureau dat veiligheid controleert. Daarnaast voorziet het beveiligingsbeleid van Blink in interne processen om kwetsbaarheden te identificeren.

Tevens worden de maatregelen volgens de BIV-classificatie waaraan niet wordt voldaan opgepakt in de volgende volgorde:

- Logging-gerelateerd (betreft Onweerlegbaarheid van gegevens en toepassing, Application controls en Logging)
- Testen (geautomatiseerd testproces)
- Software (geautomatisserd patchproces)

Overige items worden hierna opgepakt en zullen in een volgende versie van deze privacy bijsluiter worden opgenomen.

Rapportage

Verwerker rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 1 september aan Verantwoordelijke over de door Verwerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via https://mijn.blink.nl.

Indien er tussentijds vragen en of opmerkingen zijn, kan er contact worden opgenomen met Blink Onderwijssupport: 073-8500022 of onderwijssupport@blink.nl.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging:

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

  Blink monitort 24/7 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 de security officer van Blink, die analyseert of sprake kan zijn van een Datalek.

- *De wijze waarop informatie wordt gedeeld:*
  Wanneer zich een Datalek voordoet, wordt de verwerkingsverantwoordelijke onderwijsinstelling door of namens Blink in beginsel zonder onredelijke vertraging 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 mediakanalen 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.

- *Blink 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 kan Blink 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.

Versiebeheer

Deze bijlage is voor het laatst bijgewerkt op 20 januari 2022. Voor het volledige versiebeheer zie het hoofddocument.

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://www.privacyconvenant.nl.