Bijlage 1

Privacy bijsluiter Pica

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 'verantwoordelijke' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt. Blink is een 'bewerker', die uitvoering geeft aan de opdracht van een onderwijsinstelling.

De afspraken die hiervoor gelden, zijn vastgelegd in de Bewerkersovereenkomst van Blink. 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 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:	Deze Privacy Bijsluiter heeft betrekking op Pica Typen van Blink
Naam Bewerker en vestigingsgegevens:	Blink, Den Bosch. Blink is een aanbieder van (digitale) leermiddelen en educatieve diensten.
Beknopte uitleg en werking product en dienst:	Pica Typen is een digitale typecursus De volgende persoonsgegevens verwerkt. - Om toegang te krijgen tot Pica moeten gebruikers inloggen. Daarbij worden ook persoonsgegevens verwerkt. - De typecursus bevat oefenmateriaal. De gegevens die leerlingen invullen bij het gebruik van Pica, worden verwerkt door Blink om de voortgang van leerlingen te volgen. - 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.picatypen.nl
Doelgroep:	Primair Onderwijs, groep 5 t/m 8
Gebruikers:	Pica is gericht op gebruik door leerlingen, leraar, ICT-coördinator.

B. De 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, emailadres 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 onderwijstelling ook andere verwerkingen plaatsvinden. Het betreft verwerkingen in het kader van:

• het kunnen uitwisselen van leer- en testresultaten met leerling administratiesystemen (b.v. ParnasSys, Esis, Netschool) van de onderwijsinstelling;
• het bewaren van leer- en testresultaten; denk hierbij aan de opslag van gegevens van leerlingen over de jaren heen.
• extern onderzoek en analyse op basis van strikte voorwaarden zoals vastgesteld binnen het Ketenplatform van het ‘Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen’;
• de beoordeling van leer- en testresultaten om leerstof en testmateriaal te verkrijgen, dat is afgestemd op de specifieke leerbehoefte van een leerling;

C. Categorieën en soorten persoonsgegevens

Omschrijving van de verwerkte persoonsgegevens:	Het verkrijgen van toegang tot digitale leermiddelen verloopt via het platform van Pica Typen.

	Na het inloggen worden door Blink vervolgens de gegevens verwerkt die gebruikers invullen bij het gebruik van het leermiddel, zoals in een oefenopgaaf of toets. Daardoor is het bijvoorbeeld mogelijk voor een leerkracht om te zien wat ieder van zijn leerlingen met de lesstof heeft gedaan en wat het resultaat daarvan is.
Soorten van 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.

D. Algemene informatie over getroffen beveiligingsmaatregelen:

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

Persoonsgegevens worden door Blink verwerkt binnen Nederland. Een overzicht van de plaats van opslag en verwerkingen door subbewerkers die worden ingeschakeld door Blink treft u hieronder.

E. Subbewerkers

Voor de verwerking van persoonsgegevens worden door Blink subbewerkers ingeschakeld.

Naam:	Omschrijving:	Land van opslag en verwerking:	Producten:
Lab Digital	Ontwikkelaar en leverancier van het educatieve platform waarop de lesomgeving van Blink is gebaseerd	Nederland	Pica Typen

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 079 342 88 68 of via mail@picatypen.nl. Meer informatie treft u op www.picatypen.nl.

G. Versie

Deze Privacy Bijsluiter is voor het laatst bijgewerkt op 1 juli 2017.

Bijlage 2

Technische en organisatorische beveiligingsmaatregelen

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

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

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-databasebeheerders hebben toegang tot de databases	De handelingen van IT-databasebeheerders 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 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 informatiebeveiligingsafspraken gemaakt.
- Medewerkers hebben op grond van een autorisatiesystematiek 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.

Fysieke beveiliging en continuïteit van de middelen

- 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 periodiek backups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze backups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's.

Netwerk-, server- en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- De digitale leermiddelen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. Wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd op basis van patchmanagement.
- Niet (meer) gebruikte informatie wordt verwijderd.
- Op bijzondere persoonsgegevens worden zoveel mogelijk cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van de school vindt versleuteld plaats.

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.

Rapportage (artikel 7.4 van de Bewerkersovereenkomst)

Bewerker rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 1 september aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. Indien er tussentijds vragen en of opmerkingen zijn, kan er contact worden opgenomen met de Klantenservice van Pica: 079 342 88 68 of mail@picatypen.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 verantwoordelijke onderwijsinstelling door of namens Blink in beginsel binnen 24 uur na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens.

- *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.

Versie

Versie 2.0, laatst aangepast op 1 juli 2017

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: https://www.privacyconvenant.nl/.