

PRIVACY VERKLARING

I: Algemene informatie

Naam product en/of dienst:

Leesonderwijs in Beeld

Naam Verwerker en vestigingsgegevens:

Onderwijs in Beeld V.O.F.
Corleseweg 22
7102 EV, Winterswijk

Beknorte uitleg en werking product en dienst:

Het in beeld brengen van leesvaardigheid en leesplezier van leerlingen middels spraak-naar-tekst algoritmen. Zodat leerkrachten zonder extra tijdsinvestering preventief goede leesinstructie kunnen geven en beter leerlingen kunnen helpen met het kiezen van een leuk en passend boek.

Link naar leverancier en/of productpagina:

<https://onderwijsinbeeld.nl/>

Doelgroep (zoals PO/VO, onderbouw/bovenbouw):

Primair onderwijs, onderbouw en bovenbouw.

Gebruikers:

Leerlingen en leerkrachten.

II: Standaard verwerkingen

Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden basisdienstverlening door Onderwijs in Beeld.

1. Het verwerken van persoonsgegevens waaronder de leesactiviteiten van individuele leerlingen (betrokkene) voor de leerling zelf.

Onderwijs in Beeld houdt bij welke leerling welke boeken leest, wat de leerling van de boeken vindt en hoeveel bladzijden de leerling in de boeken gelezen heeft. Daarnaast verwerkt Onderwijs in Beeld leesopnames waaruit leesvaardigheid data van individuele leerlingen volgt. De resultaten worden systematisch bij elkaar opgeslagen zodat inzicht kan worden verkregen over de leesactiviteiten, de leesvaardigheidsontwikkeling en het leesplezier van de leerling.

2. Het via Leesonderwijs in Beeld beschikbaar stellen van de persoonsgegevens, waaronder de leesprestaties van de individuele leerlingen aan de leerkrachten.

Het dashboard, dat aan de Onderwijsinstelling, leerkracht en leerling ter beschikking wordt gesteld, biedt de mogelijkheid om in een oogopslag leesactiviteit, leesvaardigheidsontwikkeling en leesplezier van een leerling te zien. De administrator van de Onderwijsinstelling is verantwoordelijk voor het toebedelen van rechten aan specifieke gebruikers. Deze rechten bepalen welke gebruiker binnen het systeem de informatie van welke leerling mag inzien.

3. Het maken van een back-up

De persoonsgegevens die door Onderwijs in Beeld worden verwerkt voor de Onderwijsinstelling worden via een back-up veiliggesteld. Mocht een server van Onderwijs in Beeld uitvallen dan is het mogelijk om, na herinstallatie, door te gaan met het gebruik van Onderwijs in Beeld, met minimaal verlies van de leesprestaties.

III: Doeleinden voor het verwerken van gegevens

Onderwijs in Beeld is leverancier van een digitaal product bestaande uit leer- en toetsmiddelen. Met de verwerking van de persoonsgegevens binnen haar producten (zie onder II) ondersteunt zij de Onderwijsinstelling met bereiken van de volgende doelstellingen:

- A. Het, met gebruikmaking van Leesonderwijs in Beeld, volgen van de leesvaardigheidsontwikkeling van leerlingen door de Onderwijsinstelling en/of leerkracht en het begeleiden en volgen van onderwijsdeelnemers, waaronder:
 - de analyse en interpretatie van leesprestaties;
 - de opslag van leesprestaties;
 - het downloaden van leesprestaties door de Onderwijsinstelling;
 - het creëren van een leesprofiel aan de hand van een beoordeling van de leeshistorie en bijhorende leesinteresses.
- B. het geleverd krijgen/in gebruik kunnen nemen van Leesonderwijs in Beeld volgens de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
- C. het verkrijgen van toegang tot Onderwijs in Beeld, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
- D. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van Onderwijs in Beeld Verwerkte Persoonsgegevens.
- E. de continuïteit en goede werking van Onderwijs in Beeld volgens de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden;
- F. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
- G. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van niet direct identificeerbare cq anonieme statistische gegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
- H. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
- I. De uitvoering of toepassing van een andere wet.

IV: Categorieën en soorten persoonsgegevens

Omschrijving en opsomming categorieën betrokkenen die gebruikt worden zijn:

- 1) Leerkrachten
- 2) Leerlingen
- 3) Ondersteunend personeel

De volgende categorieën persoonsgegevens worden binnen Onderwijs in Beeld vastgelegd:

Van toepassing	Categorie	Toelichting
	1. Contactgegevens	Volledige naam, geslacht, geboortedatum, e-mail, schooljaar, klas
n.v.t.	2. Onderwijsdeelnemer nummer	een administratienummer dat onderwijsdeelnemers identificeert
	3. Nationaliteit	
n.v.t.	4. Ouders, voogd	gegevens als bedoeld onder 1, van de ouders of verzorgers van onderwijsdeelnemers
n.v.t.	5. Medische gegevens	gegevens die noodzakelijk zijn om de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
n.v.t.	6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
n.v.t.	7. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten (te weten de Studievoortgang en/of Studietraject)
n.v.t.	8. Onderwijsorganisatie	gegevens om de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
n.v.t.	9. Financiën	gegevens om het berekenen, vastleggen en innen van inschrijvingsgelden, school- en leskosten en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, en bankrekeningnummer van de betrokkene;
n.v.t.	10. Beeldmateriaal	foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;
	11. Docent, zorgcoördinator, intern begeleider, decaan, mentor	gegevens van docenten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;
	12. Overige gegevens, te weten ...	Audio-opnames van hardop lezende leerlingen en een gebruikersnummer.
n.v.t.	13. BSN/PGN	

n.v.t.	14. Keten-ID (ECK-ID)	uniek ID voor de 'educatieve contentketen'. hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.
--------	-----------------------	--

De verwerker hanteert de door de onderwijsinstelling opgegeven bewaartermijnen volgens artikel 12 uit de verwerkersovereenkomst.

V: Opslag Verwerking Persoonsgegevens

Onderwijs in Beeld en haar sub verwerkers verwerken de persoonsgegevens zoveel mogelijk binnen de Europese Unie. In enkele gevallen vindt verwerking buiten de Europese Unie plaats. Wanneer de doorgifte plaats vindt naar landen zonder een Europees passendheidsbesluit, gebeurt dit op basis van de voorgeschreven model contracten van de Europese Unie (Standard Contractual Clausses, SCC), waar nodig aangevuld met extra maatregelen om de veiligheid van de doorgifte te waarborgen.

VI: Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.

Verwerker maakt op het moment van het afsluiten van de Verwerkersovereenkomst onder andere gebruik van de volgende belangrijke Subverwerkers:

- Onderwijs in Beeld V.O.F., Winterswijk, ten behoeve van een deel van de operationele uitvoering van de Verwerkersovereenkomst (opslag EU).
- Google Cloud Services, te Amsterdam, ten behoeve van hostingactiviteiten (opslag EU) en transcriptie van audiofragmenten.

Daarnaast maakt Verwerker gebruik van enkele andere Subverwerkers (ten behoeve van "security monitoring, klantenservice, chat service, et cetera.). Een lijst van deze Subverwerkers kan worden opgevraagd via support@onderwijsinbeeld.nl.

VII: Contactgegevens

Voor vragen of opmerkingen over deze verklaring of de werking van dit product of deze dienst, kunt u terecht bij: Onderwijs in Beeld V.O.F., Corleseweg 22, 7102 EV, Winterswijk, telefoonnummer 0640545142, hallo@onderwijsinbeeld.nl of bij de Functionaris Gegevensbescherming van Onderwijs in Beeld via e-mail: support@onderwijsinbeeld.nl.

VIII: Versie Verwerkersovereenkomst

Versie 1.1, 2 juli 2021

BIJLAGE 2: TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMATREGELEN

De Verwerker is Overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Normen informatiebeveiliging

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en hoe passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.

Minimale beveiligingsmaatregelen en aantoonbaarheid

A: Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid

Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken. Onderwijs in Beeld heeft de classificatietool Certificeringsschema Informatiebeveiliging en Privacy ROSA-versie 2.01 gebruikt van Edustandaard. Jaarlijks zal deze door Onderwijs in Beeld opnieuw ingevuld worden. De uitkomst is:

- Beschikbaarheid: Hoog (3)
- Integriteit: Midden (2)
- Vertrouwelijkheid: Hoog (3)

B: Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan

- I. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast. Uitgangspunt van dit beleid is de EDU standaard ROSA welke gebaseerd is op de ISO-standaarden 27001 en 27002;
- II. Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- III. Onderwijs in Beeld heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.
- IV. Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt. Onderwijs in Beeld stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging en privacy. Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
- V. Met betrekking tot de beschikbaarheid van data heeft Onderwijs in Beeld o.a. de volgende maatregelen getroffen:
 - a. Overbelasting; actieve monitoring gebruikersverkeer
 - b. Business Continuity: cold stand-by waarbij gewerkt wordt aan implementatie van een warm stand-by.
 - c. Ontwerp; Gedurende de ontwerpfase worden de essentiële afhankelijkheden meegenomen en getest.
 - d. Monitoring: continue monitoring met alert.
 - e. Testen: Gedurende de ontwikkeling vinden unit, integratie en end-to-end tests.
 - f. Software: Periodieke monitoring op noodzakelijke patches en uitgevoerd.
 - g. Actuele dreigingen: DDOS-alerting ingericht gecombineerd met firewalls.

VI. Met betrekking tot Integriteit van de data heeft Onderwijs in Beeld o.a. de volgende maatregelen getroffen:

- a. Herleidbaarheid: Monitoring op de essentiële velden in de applicatie.
- b. Back-up: Dagelijks volledig en incrementeel per uur (RPO 1 uur).
- c. Application controls: invoer controles zijn ingericht op essentiële velden.
- d. Onweerlegbaarheid: Logging is actief ingevoerd met daarbij tijdige alerts en opvolging.
- e. Herleidbaarheid: Onderwijs in Beeld werkt alleen met unieke user ID's.
- f. Controle integriteit: antivirus, malware inrichting, patch management en secure coding in het ontwikkelproces.
- g. Onweerlegbaarheid: configuratie wijzigen worden gelogd en automatisch gemonitord.
- h. Actuele dreigingen: RPO van 1 uur bij ransomware en bewustwordingscampagnes.

VII. Met betrekking tot vertrouwelijkheid van de data heeft Onderwijs in Beeld de o.a. de volgende maatregelen getroffen:

- a. Levenscyclus gegevens: operationele processen zijn ingericht om op verzoek data te kunnen vernietigen. E.a. zal in de toekomst geautomatiseerd worden.
- b. Logische toegang: user access beleid gebaseerd op role-based access, sterke wachtwoorden en periodieke vernieuwing, gecombineerd met multi-factor authenticatie waar nodig.
- c. Fysieke toegang: uitbesteed aan Google waar de hoogste normen gelden.
- d. Netwerk toegang: netwerk segmentatie gecombineerd met whitelisting voor IP-adressen en firewalls.
- e. Scheiding omgevingen: ingericht gecombineerd met adequate user access, in testomgeving wordt gebruik gemaakt van gepseudonimiseerde testdata
- f. Transport en Fysieke opslag: Alla data wordt buiten het datacentrum geencrypt zowel in transport als in opslag. Dit is wel afhankelijk van de hardware gebruikt door de onderwijsinstellingen.
- g. Logging: De toegang tot de essentiële velden wordt gelogd en gemonitord.
- h. Toetsing: De data in de systemen zijn geclassificeerd en periodiek vindt er een risico/dreigingen analyse plaats. Ondersteund door vulnerability scanning en pentests.
- i. Actuele dreigingen: Logging, periodiek wijzigingen van VPN-certificaten, awareness activiteiten en datalekprocedure.

C: Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging

Jaarlijks toetst Onderwijs in Beeld de classificatie en de opzet en bestaan van de daarmee samenhangende getroffen maatregelen aan de Certificeringsschema informatiebeveiliging en privacy ROSA. Noodzakelijke acties worden geïdentificeerd en geprioriteerd om een passende informatiebeveiliging van de aan Onderwijs in Beeld toevertrouwde persoonsgegevens te waarborgen.

D: Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: Onderwijs in Beeld V.O.F., Corleseweg 22, 7102 EV, Winterswijk, telefoonnummer 0640545142, bereikbaar maandag t/m vrijdag van 09.00 tot 17.00 uur. Buiten deze tijden kunt u contact opnemen met: support@onderwijsinbeeld.nl.

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

Onderwijs in Beeld hanteert een vast protocol voor meldingen van datalekken en/of incidenten. Onderwijs in Beeld zal altijd de FG (bij afwezigheid de directie) van de Onderwijsinstelling informeren, binnen maximaal 24 uur na constatering van datalekken of een beveiligingsincident.

Onderwijs in Beeld heeft een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat tenminste de volgende punten:

- De manier waarop monitoring en identificatie van incidenten plaatsvindt,
- De manier waarop informatie wordt gedeeld (via e-mail, telefoon):
- Wie wordt geïnformeerd (contactpersonen en contactgegevens); - Met wie Onderwijs in Beeld (bij vervolgacties) contact opneemt.
- Informatie die in ieder geval over een incident gedeeld wordt
 - a) 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);
 - b) De oorzaak van het beveiligingsincident;
 - c) De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
 - d) Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
 - e) De omvang van de groep betrokkenen;
 - f) 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).
- Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.