

BIJLAGE 1: PRIVACY BIJSLUITER ABAS

Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals bv. leerlingen en leerkrachten). De Verwerkingsverantwoordelijken moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiters geeft Onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar gaat het over de vragen gegevens van de betrokken personen verwerkt en waar, waarom en hoe deze gegevens worden verwerkt

Het gebruik van deze Privacy Bijsluiters helpt de Verwerkingsverantwoordelijken (en dus ook de Onderwijsinstellingen) om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. Op basis van deze bijsluiters kan een register van verwerkingsactiviteiten verder ingevuld en onderhouden worden.

In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van deze Privacy Bijsluiters. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in aparte Bijlage(n), welke als volgt

Verwerkersovereenkomst gehecht.

A. Algemene informatie

Naam product en/of dienst:	Kabas (www.kabas.be)
Naam Verwerker en vestigingsgegevens:	Die Keure N.V., Kleine Pathoekeweg 3, 8000 Brugge
Beknopte uitleg over werking product en dienst:	Kabas is een onderwijsplatform voor leerkrachten en leerlingen. Leerkrachten kunnen lesmateriaal raadplegen, opdrachten geven en resultaten inkijken. Leerlingen kunnen oefeningen maken.
Link naar aanbieder en/of productpagina:	www.diekeure.be www.kabas.be
Doelgroep:	Basisonderwijs
Gebruikers:	Leerlingen en leerkrachten

B. Algemene informatie betreffende de Verwerkingen

Onderwerp van de Verwerking(en):	Diensten die in de Product- en Dienstenovereenkomst uiteengezet worden, zie algemene voorwaarden op www.kabas.be
---	--

Duur van de Verwerking(en):	Gegevens van leerlingen worden bijgehouden tot 6 jaar na het zesde leerjaar, tenzij de school deze eerder verwijdert.
Aard van de Verwerking(en):	Terbeschikkingstelling van, en mogelijkheid tot wijzigingen aan, gegevens voor het leveren van het product en de diensten die in de Product- en Dienstenovereenkomst uiteengezet worden
Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen	<p>Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst:</p> <ul style="list-style-type: none"> • Naam van alle gebruikers wordt opgeslagen en verwerkt om tot een efficiënt gebruik van Kabas te komen. Zo kunnen leerkrachten de resultaten per leerling bekijken en kunnen zij differentiëren bij het toekennen van oefeningen. • Stamnummer binnen een school wordt opgeslagen om een leerling uniek te identificeren binnen een school en via excell import van klas te laten veranderen. • IP adres wordt opgeslagen en verwerkt voor rapporteringsdoeleinden. • Email-adres van leerkrachten wordt opgeslagen voor inhoudelijke ondersteuning (leerkrachten kunnen een lijst ontvangen met resultaten op hun emailadres), voor directe marketing, en voor het beheer van de account.

C. Doeleinden

Doel:

Leermiddelen verstrekken of ter beschikking stellen voor het geven en volgen van onderwijs waaronder:

- de opslag van leer- en toetsresultaten;
- het terug ontvangen door de Onderwijsinstelling van leer- en toetsresultaten;
- de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een leerling (o.a. adaptief lesmateriaal);
- analyse en interpretatie van leerresultaten;
- het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.

Het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Verwerker waaronder:

- het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen (identificatie, authenticatie en autorisatie);

- de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens;
- de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier (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...).

D. Categorieën Persoonsgegevens en bewaartermijnen

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:

- Administratieve gegevens: bv. naam, adres, e-mailadres, inloggegevens,...
- Gegevens betreffende de kennis, prestatie, vaardigheden

Bewaartermijnen van de Persoonsgegevens:

Gegevens worden bijgehouden tot 6 jaar na het 6de leerjaar, tenzij de school deze eerder verwijdert.

E. Categorieën van betrokkenen

- Leerlingen/cursisten en personen die ouderlijk gezag over de leerlingen uitoefenen of in rechte of in feite de minderjarige onder hun bewaring hebben
- Personeel en medewerkers

F. Opslag van de persoonsgegevens:

Plaats/land van opslag en Verwerking van de Persoonsgegevens:	EU/Ierland
---	------------

G. Subverwerkers

Verwerker maakt voor dienst/product gebruik van de volgende Subverwerkers:

Naam:	Omschrijving:	Plaats/land van opslag en Verwerking:
AWS	Hosting provider voorziet in de database waar alle persoonsgegevens in worden opgeslagen.	EU/Ierland

Adaptemy.IO	Verwerking van persoonsgegevens voor interne analytische doeleinden. Alle persoonsgegevens zijn evenwel geanonimiseerd en dus niet herleidbaar tot een persoon	EU / Ierland
Google Analytics	IP adres wordt verwerkt voor interne analytische doeleinden teneinde onze service te verbeteren voor scholen.	EU

H. Contactgegevens

kabas@diekeure.be

I. Versie _____versie 29 september 2021

BIJLAGE 2: Algemene Technische en organisatorische beveiligingsmaatregelen

Volgens artikel 28.1 van de AVG doet de Verwerkersverantwoordelijke uitsluitend een beroep op Verwerkers die afdoende garanties m.b.t. technische en organisatorische maatregelen bieden zodat Persoonsgegevens voldoende beschermd zijn en de rechten van de Betrokkene gewaarborgd blijven.

Volgens artikel 32 van de AVG moet de Verwerker passende technische en organisatorische maatregelen nemen ter beveiliging van de Verwerking van Persoonsgegevens.

In deze bijlage geven Verwerkers aan wat hun algemene technische en organisatorische beveiligingsmaatregelen zijn zodat Verwerkingsverantwoordelijke voldoende garanties krijgt inzake beveiliging van Persoonsgegevens.

Algemene omschrijving van de maatregelen zoals bedoeld in artikel 6.2 van de Verwerkersovereenkomst

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

Enkel bevoegd personeel heeft toegang tot de persoonsgegevens die verwerkt worden bij die Keure. Er is een fysieke toegangscontrole voor de gebouwen van de medewerkers. Derden kunnen niet zonder autorisatie en begeleiding de gebouwen betreden.

De toegang tot de systemen binnen die Keure kan enkel gebeuren na goedkeuring door een geautoriseerde persoon. Er wordt gecontroleerd of de vraag tot toegang nodig en relevant is alvorens goedkeuring te geven.

De toegang tot de persoonsgegevens bij de sub-verwerkers (hosting bedrijven) is eveneens onderhevig aan minimaal dezelfde eisen. De hostingbedrijven waar die Keure mee samenwerkt maken oa. gebruik van fysieke toegangscontrole, fysieke beveiligingssystemen, beveiligingspersoneel ter plaatste, camerabeveiliging.

II. Algemene 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.

Een operationeel manager dient de aanvraag voor toegang tot persoonsgegevens goed te keuren.

Toegang tot de systemen is enkel mogelijk via interne toestellen. Toestellen die niet op een lijst van geverifieerde toestellen staan zullen geen toegang kunnen krijgen tot het systeem.

Bij personeel is het is niet toegestaan om accounts te delen, net zoals ook bij de gebruikers van het systeem.

Aan iedere eindgebruiker is een aparte account gekoppeld, zodat er traceerbaarheid is van alle events die gelogd zijn via een eindgebruiker/account.

Binnen die Keure en bij de sub-verwerkers is voor personeelsleden via het arbeidsreglement de geheimhouding schriftelijk overeengekomen.

Alleen adequaat personeel kan toegang krijgen tot de persoonsgegevens. Waar nodig wordt er ook een onderscheid gemaakt tussen personeel die toegang krijgt tot ontwikkel, test en productie-omgeving.

III. Algemene omschrijving rond het informatieveiligheidsbeleid en de maatregelen om zwakke plekken te identificeren en aan te pakken ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

Computers en laptops zijn beschermd door anti-malware oplossingen die met grote regelmaat updates ontvangen van nieuwe definities.

Indien er zich grote probleem voordoen dan wordt een major incident team ingericht om zo snel mogelijk de oorzaak van het probleem te achterhalen, evenals toekomstige herhaling van het probleem.

Informereren over Inbreuken in verband met persoonsgegevens

Het informeren in geval van Inbreuken in verband met persoonsgegevens en/of incidenten met betrekking tot beveiliging. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de onderstaande informatie zonder onredelijke vertraging in stappen worden verstrekt.

- Informatie die in ieder geval over een incident gedeeld moet worden zodat de Verwerkingsverantwoordelijke aan de meldplicht aan de Gegevensbeschermingsautoriteit kan voldoen. De vetgedrukte elementen moeten zeker worden meegedeeld ingeval van een inbreuk in verband met persoonsgegevens.
 - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en **aard incident** (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 het incident aan te pakken en eventuele/verdere schade te beperken en 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);

- De **omvang van de gegevens**;
- De **waarschijnlijke gevolgen voor de betrokkene**.

Versie

Versie 1.0

september 2021