Bernadet.

DIGITAAL STAGECONTRACTPLATFORM

Verwerkersovereenkomst

Laatst bijgewerkt: 07/10/2026

Data Processing Agreement (DPA) conform artikel 28 AVG · versie 2.0 · 7 oktober 2026

> Deze verwerkersovereenkomst vormt een integraal onderdeel van de dienstverleningsovereenkomst tussen de school en de verwerker. Een wederzijds ondertekend exemplaar kan gedownload, ondertekend en teruggestuurd worden volgens artikel 17.

1. Partijen

Deze verwerkersovereenkomst (hierna "DPA") wordt gesloten tussen:

- **De verwerkingsverantwoordelijke:** de onderwijsinstelling die het Bernadet.-platform inzet voor het beheer van stageovereenkomsten. De school bepaalt het doel en de middelen van de verwerking van persoonsgegevens.

De verwerker:

> **Jacobs, Axel** — handelend onder commerciële benaming **Molokini**
>
> Eenmanszaak
>
> KBO-nummer: BE 0896.293.658
>
> Maatschappelijke zetel: Sint-Katharinavest 56, 1500 Halle, België
>
> Contact: axel@molokini.be

Hierna aangeduid als "de verwerker". De verwerker verwerkt persoonsgegevens uitsluitend namens en in opdracht van de verwerkingsverantwoordelijke.

2. Voorwerp en duur

Deze DPA is van toepassing op alle verwerkingen van persoonsgegevens die de verwerker uitvoert in het kader van het Bernadet.-platform.

De DPA geldt voor de volledige duur dat de verwerkingsverantwoordelijke het Platform gebruikt en wordt automatisch verlengd bij voortgezet gebruik. De DPA eindigt op het moment dat alle persoonsgegevens zijn teruggegeven of gewist conform artikel 11 van deze overeenkomst.

De DPA hangt onlosmakelijk samen met de dienstverleningsovereenkomst en kan niet los daarvan worden opgezegd. Bepalingen die uit hun aard bedoeld zijn om na het einde van de overeenkomst voort te duren (waaronder geheimhouding, bijstand, vernietiging en aansprakelijkheid) blijven van kracht.

De bijlagen 1 tot en met 3 maken integraal deel uit van deze DPA en volgen de structuur van het in het Vlaamse onderwijs gebruikelijke model van verwerkersovereenkomst.

3. Aard en doel van de verwerking

De verwerking heeft als doel het digitaal beheer van stageovereenkomsten in opleidingscontext, en omvat de volgende activiteiten:

- Het aanmaken, bewerken, ondertekenen en archiveren van stagecontracten
- Het registreren en goedkeuren van urenstaten
- Het bijhouden van een stagekalender (werkdagen, afwezigheden, vakanties)
- Het uitvoeren van evaluaties door stagebegeleiders en stagementoren
- Het faciliteren van digitale handtekeningen met IP-registratie
- Het verzenden van notificaties en herinneringen per e-mail
- Het genereren van PDF-documenten (contracten, urenstaten, attesten)
- Het bijhouden van een audit trail (activiteitenlogboek)

4. Type persoonsgegevens

De volgende categorieën persoonsgegevens worden verwerkt:

- **Identificatiegegevens:** naam, e-mailadres, telefoonnummer, studentnummer
- **Adresgegevens:** straat, postcode, stad
- **Geboortedatum**
- **Opleidingsgegevens:** school, campus, opleiding, academiejaar

- **Stagegegevens:** stagegever, vestiging, mentor, begeleider, contractstatus, stageperiode
- **Urenstaten:** gewerkte uren, beschrijvingen, goedkeuringsstatus
- **Evaluatiegegevens:** beoordelingen door mentor en begeleider
- **Gezondheidsgegevens (bijzondere categorie, Art. 9 AVG):** doktersattesten bij ziekteverzuim — worden automatisch verwijderd 3 maanden na goedkeuring
- **Technische gegevens:** IP-adres bij digitale ondertekening, inlogactiviteit

5. Categorieën betrokkenen

- **Studenten** (mogelijk minderjarig — in dat geval bevestigt een ouder of voogd één keer zijn of haar akkoord; dat akkoord is geen rechtsgrond in de zin van de AVG)
- **Stagebegeleiders** (personeelsleden van de school)
- **Stagementoren** (contactpersonen bij stagegevers)
- **Schoolbeheerders en campusbeheerders**
- **Stagegeverbeheerders en vestigingscontactpersonen**
- **Ouders of voogden** (beperkt tot het e-mailadres, het tijdstip en het IP-adres van het akkoord, en — als de school de ouderhandtekening vereist — getypte naam, e-mailadres, tijdstip en IP-adres van hun handtekening onder het stagecontract; en, als zij een opmerking bij het contract sturen, hun getypte naam, de tekst van de opmerking en hun IP-adres)

6. Verplichtingen van de verwerker

De verwerker verbindt zich ertoe:

- **Instructies:** persoonsgegevens uitsluitend te verwerken op basis van gedocumenteerde instructies van de verwerkingsverantwoordelijke, tenzij een wettelijke verplichting anders voorschrijft. Meent de verwerker dat een instructie in strijd is met de AVG of andere regelgeving, dan licht hij de verwerkingsverantwoordelijke daarover onverwijld in.
- **Doelbinding:** persoonsgegevens niet te gebruiken voor andere doeleinden of op andere wijze dan waarvoor ze zijn verstrekt, zowel tijdens als na afloop van de overeenkomst. De doeleinden en de categorieën persoonsgegevens staan in artikel 3, artikel 4 en bijlage 1.
- **Geen verstrekking aan derden:** geen persoonsgegevens aan een derde te verstrekken, tenzij (a) dit gebeurt in opdracht van of met uitdrukkelijke toestemming van de verwerkingsverantwoordelijke, (b) de betrokkene (of diens ouders of wettelijk

vertegenwoordiger) zelf aangeeft dat de gegevens aan een derde mogen worden verstrekt, of (c) dit noodzakelijk is om te voldoen aan een wettelijke verplichting. In dat laatste geval controleert de verwerker vooraf de grondslag van het verzoek en de identiteit van de verzoeker, en informeert hij de verwerkingsverantwoordelijke onmiddellijk, zo mogelijk vóór de verstrekking, voor zover de wet dat toelaat.

- **Vertrouwelijkheid:** ervoor te zorgen dat alle personen die gemachtigd zijn persoonsgegevens te verwerken, onder wie werknemers, vertegenwoordigers en subverwerkers, gebonden zijn aan een geheimhoudingsplicht of aan een passende wettelijke verplichting van vertrouwelijkheid. Die geheimhouding geldt zowel tijdens als na afloop van de overeenkomst.
- **Register en toezicht:** een register bij te houden van alle categorieën van verwerkingsactiviteiten die hij ten behoeve van de verwerkingsverantwoordelijke verricht (art. 30 lid 2 AVG), en desgevraagd mee te werken met de toezichthoudende autoriteiten.
- **Beveiliging:** passende technische en organisatorische maatregelen te treffen, waaronder:
  - Versleutelde verbindingen (HTTPS/TLS)
  - Rolgebaseerde toegangscontrole (6 rollen met specifieke rechten)
  - Audit trail (activiteitenlogboek van alle wijzigingen)
  - Rate limiting op gevoelige endpoints
  - Wachtwoordbeleid en e-mailverificatie
  - CSRF-bescherming op alle formulieren
  - Gesigneerde URL's voor gevoelige acties (wachtwoord instellen, toestemmingslinks)
  - Versleuteling-at-rest van bijzondere-categorie gegevens (doktersattesten, geboortedatum) via Laravel encryption casts
  - Dagelijkse versleutelde systeemback-ups van de productieomgeving binnen de EER (datacenter Amsterdam, 7 dagen retentie), conform het interne backup-beleid (zie referentie hieronder)

  Als referentiekader hanteert de verwerker het zekerheidsniveau "Basis" van het Cyber Fundamentals Framework van het Centre for Cybersecurity Belgium (CCB). Bijlage 3 geeft per onderdeel weer wat reeds is geïmplementeerd en wat nog gepland is, met een tijdpad; die tabel geldt als contractuele verbintenis. De verwerker houdt dat overzicht actueel, evalueert zijn informatiebeveiligingsbeleid en -maatregelen minstens jaarlijks en bij belangrijke wijzigingen, en houdt rekening met de stand van de techniek.

- **DPIA:** de verwerker heeft een gegevensbeschermingseffectbeoordeling (DPIA) conform artikel 35 AVG uitgevoerd voor de verwerkingsactiviteiten binnen het Platform. Het DPIA-rapport is op verzoek beschikbaar voor de verwerkingsverantwoordelijke.
- **Backup-beleid:** de verwerker hanteert een gedocumenteerd backup-beleid. Operationeel zijn dagelijkse, versleutelde systeemback-ups van de productieomgeving binnen de EER (DigitalOcean, datacenter Amsterdam, 7 dagen retentie). Het beleid voorziet daarnaast in een kwartaalgewijze restore-verificatie. Een onafhankelijke off-site replicatie bij een tweede EER-provider wordt gefaseerd ingevuld. Het beleid is op verzoek beschikbaar.
- **Bijstand AVG-rechten:** de verwerkingsverantwoordelijke bij te staan bij het beantwoorden van verzoeken van betrokkenen (inzage, rectificatie, wissing, overdraagbaarheid). Het Platform biedt hiervoor een ingebouwde functie ("Mijn gegevens (AVG)") waarmee betrokkenen hun gegevens kunnen inzien en exporteren. Een klacht of verzoek dat rechtstreeks bij de verwerker binnenkomt, stuurt de verwerker onverwijld door naar de verwerkingsverantwoordelijke, die de verdere afhandeling op zich neemt.
- **Aantonen van naleving:** de verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de naleving van artikel 28 AVG en van deze DPA aan te tonen, bijvoorbeeld via rapportages, de DPIA of een gelijkwaardig bewijsmiddel.

7. Subverwerkers

De verwerkingsverantwoordelijke geeft hierbij algemene toestemming aan de verwerker om subverwerkers in te schakelen. De verwerker maakt momenteel gebruik van de volgende subverwerkers:

Subverwerker	Doel	Verwerkingslocatie	Doorgiftewaarborg
DigitalOcean, LLC	Hosting van de applicatie en de database (cloudserver)	Datacenter Amsterdam (EER); onderneming VS	Data-at-rest in EER-datacenter (Amsterdam, AMS3). DigitalOcean is gecertificeerd onder het EU-US Data Privacy Framework en hanteert Standaardcontractbepalingen (SCC) voor eventuele toegang vanuit de VS.

Subverwerker	Doel	Verwerkingslocatie	Doorgiftewaarborg
Resend, Inc.	Verzending van transactionele e-mail (contractmeldingen, herinneringen, wachtwoord-reset)	VS (aflevering via AWS-datacenter Ierland)	EU-US Data Privacy Framework-certificering en Standaardcontractbepalingen (SCC). De e-mailinhoud bevat enkel naam en e-mailadres van de ontvanger; geen bijzondere categorieën van gegevens.
Functional Software, Inc. (Sentry)	Registratie van applicatiefouten voor incident-respons (foutmonitoring)	EU-region (Frankfurt); onderneming VS	Verwerking in de EU-region (Frankfurt) met persoonsgegevensverzameling uitgeschakeld (geen IP-adressen, request-headers of gebruikersdata). EU-US Data Privacy Framework en Standaardcontractbepalingen (SCC).
Microsoft Ireland Operations Ltd	Single sign-on via Microsoft 365 / Azure AD (optioneel, enkel indien de school dit activeert)	Ierland (EER)	Gevestigd binnen de EER. Wordt uitsluitend ingeschakeld wanneer de school single sign-on activeert.
Google Ireland Limited	Single sign-on via Google Workspace (optioneel, enkel indien de school dit activeert)	Ierland (EER); moederonderneming VS	EU-US Data Privacy Framework en Standaardcontractbepalingen (SCC). Wordt uitsluitend ingeschakeld wanneer de school single sign-on activeert.

De productiegegevens (applicatie en database) worden opgeslagen in een datacenter binnen de Europese Economische Ruimte (Amsterdam). Een aantal subverwerkers is een in de Verenigde Staten gevestigde onderneming of heeft een Amerikaanse moederonderneming; voor die subverwerkers gelden de in de tabel vermelde doorgiftewaarborgen (zie ook artikel 8).

De verwerker legt aan elke subverwerker, via een overeenkomst of andere rechtshandeling, minstens dezelfde verplichtingen inzake gegevensbescherming op als die in deze DPA, en houdt de lijst hierboven actueel.

De verwerker informeert de verwerkingsverantwoordelijke ten minste 30 dagen vooraf over elke voorgenomen toevoeging of vervanging van een subverwerker. De kennisgeving vermeldt minstens

de naam en contactgegevens van de subverwerker, de taak of dienst, de categorieën persoonsgegevens, de plaats van opslag en verwerking en, in voorkomend geval, de doorgiftegrond.

De verwerkingsverantwoordelijke kan binnen 30 dagen na de kennisgeving schriftelijk en gemotiveerd bezwaar maken. Het bezwaar is ontvankelijk als het gegrond is op een of meer van deze redenen: (a) de subverwerker biedt onvoldoende garanties voor passende technische en organisatorische maatregelen, (b) de doorgiftegrond is ontoereikend of niet rechtsgeldig, of (c) er zijn concrete indicaties dat de inschakeling een inbreuk oplevert op de AVG of andere regelgeving inzake gegevensbescherming. Zonder bezwaar binnen die termijn geldt de wijziging als aanvaard.

Na een gemotiveerd bezwaar heeft de verwerker 30 dagen om aan te tonen dat het bezwaar ongegrond is, bijkomende maatregelen voor te stellen of een alternatieve subverwerker aan te bieden. Is er na die termijn geen oplossing die het bezwaar redelijkerwijs ondervangt, dan geldt: (i) is de subverwerker beperkt tot een afgebakende functionaliteit van het Platform, dan wordt enkel die functionaliteit opgeschort tot een aanvaardbare oplossing is gevonden; (ii) is de subverwerker onlosmakelijk verbonden met de kern van het Platform, dan mag de verwerkingsverantwoordelijke deze DPA en de dienstverleningsovereenkomst beëindigen, met een opzegtermijn van maximaal 3 maanden waarin de dienstverlening en de overstap conform artikel 11 verzekerd blijven.

8. Doorgifte buiten de EER

De persoonsgegevens worden opgeslagen en primair verwerkt binnen de Europese Economische Ruimte (EER). De applicatie en de database draaien op een server in een datacenter te Amsterdam (Nederland). E-mailverzending verloopt via een afleverdatacenter in Ierland.

Een beperkt aantal subverwerkers (zie artikel 7) is echter een in de Verenigde Staten gevestigde onderneming of heeft een Amerikaanse moederonderneming. Hierdoor kan in theorie sprake zijn van een doorgifte van persoonsgegevens naar de Verenigde Staten in de zin van hoofdstuk V van de AVG. Voor elke dergelijke doorgifte zijn passende waarborgen voorzien:

- **EU-US Data Privacy Framework:** de betrokken subverwerkers (DigitalOcean, Resend, Sentry en Google) zijn gecertificeerd onder het door de Europese Commissie bij adequaatheidsbesluit van 10 juli 2023 erkende EU-US Data Privacy Framework.
- **Standaardcontractbepalingen (SCC):** aanvullend zijn met deze subverwerkers de door de Europese Commissie vastgestelde modelcontractbepalingen (Uitvoeringsbesluit (EU) 2021/914) gesloten, als bijkomende waarborg.
- **Aanvullende technische maatregelen:** de gegevens worden at-rest opgeslagen in de EER (Amsterdam); foutmonitoring (Sentry) gebeurt in de EU-region (Frankfurt) met

persoonsgegevensverzameling uitgeschakeld; e-mailverkeer beperkt zich tot naam en e-mailadres.

De verwerker geeft géén bijzondere categorieën van persoonsgegevens (waaronder de doktersattesten bedoeld in artikel 4) door buiten de EER: deze worden uitsluitend opgeslagen en verwerkt op de EER-server. Bij elke voorgenomen nieuwe doorgifte buiten de EER licht de verwerker de verwerkingsverantwoordelijke vooraf in conform artikel 7.

Verificatie en monitoring van de doorgiftegrond. De verwerker controleert minstens jaarlijks per betrokken subverwerker of de doorgiftegrond geldig blijft: bij het EU-US Data Privacy Framework of de subverwerker nog actief gecertificeerd is (te raadplegen op dataprivacyframework.gov) en welke categorieën persoonsgegevens de certificering dekt; bij standaardcontractbepalingen of de gebruikte versie nog overeenstemt met de actuele modelbepalingen. De verwerker informeert de verwerkingsverantwoordelijke onverwijld bij intrekking, schorsing, vernietiging of niet-verlenging van een adequaatheidsbesluit of van een certificering, of bij elke andere omstandigheid waardoor de doorgiftegrond niet langer rechtsgeldig is.

In dat geval voorziet de verwerker binnen 30 dagen in een alternatieve doorgiftegrond. Lukt dat niet, dan wordt de doorgifte aan *die subverwerker* opgeschort; de overige onderdelen van de dienstverlening blijven bestaan, voor zover technisch mogelijk.

Staving. Bij doorgifte op basis van standaardcontractbepalingen kan de verwerker op verzoek van de school, het schoolbestuur of hun functionaris voor gegevensbescherming de gesloten contractbepalingen en de publiek beschikbare documentatie van de subverwerker over de doorgiftemaatregelen voorleggen. Meent de verwerkingsverantwoordelijke op basis daarvan dat de doorgifte onvoldoende waarborgen biedt, dan geldt de bezwaarprocedure van artikel 7.

9. Bijstand aan de verwerkingsverantwoordelijke

De verwerker staat de verwerkingsverantwoordelijke bij in het nakomen van diens verplichtingen onder de AVG, waaronder:

- De beveiliging van de verwerking (art. 32 AVG)
- Het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) indien nodig
- Voorafgaande raadpleging van de Gegevensbeschermingsautoriteit (GBA) indien nodig
- Het beantwoorden van verzoeken van betrokkenen tot uitoefening van hun rechten, binnen de wettelijke termijnen (art. 12 tot en met 23 AVG)

De bijstand gebeurt rekening houdend met de aard van de verwerking en de informatie waarover de verwerker beschikt.

10. Datalekprocedure

In geval van een inbreuk in verband met persoonsgegevens (datalek) zal de verwerker de verwerkingsverantwoordelijke hiervan zonder onredelijke vertraging en uiterlijk binnen **72 uur** na kennisname op de hoogte stellen, conform artikel 33 AVG. Is een hoog risico voor de rechten en vrijheden van natuurlijke personen te vermoeden, dan gebeurt de melding onverwijld.

De melding bevat ten minste:

- Een beschrijving van de aard van het datalek, met vermelding van de categorieën en het geschatte aantal betrokkenen en persoonsgegevens
- De naam en contactgegevens van het aanspreekpunt voor meer informatie
- Een beschrijving van de waarschijnlijke gevolgen van het datalek
- Een beschrijving van de maatregelen die zijn genomen of worden voorgesteld om het datalek te verhelpen en de nadelige gevolgen te beperken

Is het niet mogelijk om alle informatie gelijktijdig te verstrekken, dan wordt ze zonder onredelijke vertraging in stappen aangevuld. Bijlage 2 bevat de afspraken over de inhoud van die meldingen.

De verwerkingsverantwoordelijke is verantwoordelijk voor de eventuele melding van het datalek aan de GBA en aan de betrokkenen. De verwerker stelt hem daarvoor in staat passende vervolgstappen te nemen en staat hem op verzoek bij en adviseert hem. De verwerkingsverantwoordelijke vraagt die hulp pas wanneer hij zelf niet over de nodige informatie beschikt om zijn wettelijke verplichtingen na te komen.

Beide partijen nemen zo spoedig mogelijk alle redelijkerwijs nodige maatregelen om (verdere) schending te voorkomen of te beperken, en houden een overzicht bij van de incidenten en de genomen maatregelen. Op verzoek verleent de verwerker de verwerkingsverantwoordelijke daarin inzage.

11. Teruggave en verwijdering van gegevens

Tijdens de looptijd hanteert de verwerker de bewaartermijnen uit de Privacyverklaring en bijlage 1: actieve contracten worden bewaard zolang nodig, gearchiveerde contracten tot 10 jaar, verwijderde accounts worden definitief gewist na 2 jaar.

Export en overstap. Om continuïteit te waarborgen en afhankelijkheid van één leverancier te vermijden:

- De verwerkingsverantwoordelijke kan te allen tijde, en uiterlijk bij beëindiging, een volledige export opvragen van alle gegevens die in zijn opdracht worden verwerkt. Het Platform biedt hiervoor een ingebouwde exportfunctie in een gestructureerd, gangbaar en machineleesbaar formaat (JSON), met behoud van de samenhang van de gegevens (bijlage 1, onderdeel H).
- De verwerker rekent geen kosten aan voor de extractie of overdracht van de gegevens.
- Gedurende een overgangsperiode van minstens 30 dagen na opzegging verleent de verwerker de nodige technische bijstand voor de migratie naar een andere aanbieder of een eigen systeem, en blijft de dienstverlening beschikbaar tegen de voorwaarden en de vergoeding van de dienstverleningsovereenkomst.

Vernietiging. Na de export, na het verstrijken van de bewaartermijn of bij beëindiging van de dienstverleningsovereenkomst wist de verwerker alle persoonsgegevens die in opdracht van de verwerkingsverantwoordelijke worden verwerkt, binnen 30 dagen, tenzij bewaring wettelijk verplicht is. Gegevens in systeemback-ups verdwijnen daarna door de rotatie van die back-ups (7 dagen). De verwerker bevestigt de vernietiging schriftelijk of elektronisch.

De verplichtingen in dit artikel gelden voor zover de intellectuele eigendom van de gegevens, de sjablonen of de werking van het Platform dat toelaat. De intellectuele eigendom op het Platform zelf blijft bij de verwerker.

12. Audit

De verwerkingsverantwoordelijke heeft het recht om audits of inspecties uit te voeren, of te laten uitvoeren door een onafhankelijke auditor, om de naleving van deze DPA te controleren.

De verwerker stelt alle noodzakelijke informatie ter beschikking en verleent medewerking. Audits gebeuren op kosten van de verwerkingsverantwoordelijke, worden minstens 15 werkdagen vooraf aangekondigd en vinden plaats op een in onderling overleg bepaald tijdstip. Ze zijn beperkt tot één audit per kalenderjaar, tenzij een datalek of concrete aanwijzingen van niet-naleving een bijkomende audit rechtvaardigen. De auditor is gebonden door vertrouwelijkheid en krijgt geen toegang tot gegevens van andere verwerkingsverantwoordelijken.

De verwerker rekent geen kosten aan voor zijn redelijke medewerking, tot maximaal 4 uur per audit; bijkomende tijd mag tegen het gebruikelijke tarief worden aangerekend. Een DPIA (art. 35 AVG) op initiatief van de verwerkingsverantwoordelijke geldt als audit in de zin van dit artikel.

13. Aansprakelijkheid

De aansprakelijkheid van partijen is geregeld conform artikel 82 AVG. Elke partij is aansprakelijk voor de schade die het gevolg is van een verwerking die in strijd is met de AVG.

De verwerker is enkel aansprakelijk voor schade die is veroorzaakt door een verwerking die niet voldoet aan de specifieke verplichtingen van de AVG voor verwerkers, of die in strijd is met de instructies van de verwerkingsverantwoordelijke. Een partij die de schade geheel heeft vergoed, kan het deel van de schade dat overeenkomt met de aansprakelijkheid van een andere betrokken verwerkingsverantwoordelijke of verwerker op die partij verhalen (art. 82 lid 5 AVG).

Dit artikel doet geen afbreuk aan de rechten van betrokkenen onder artikel 82 AVG. Tussen partijen blijven de aansprakelijkheidsbeperkingen van de Algemene Voorwaarden en de licentieovereenkomst van toepassing, voor zover wettelijk toegelaten.

14. Privacy-contactpunt en Functionaris Gegevensbescherming

De verwerker heeft **geen formele Functionaris Gegevensbescherming (DPO)** aangesteld. Op grond van artikel 37.1 AVG is een DPO-aanstelling enkel verplicht wanneer (a) de verwerking plaatsvindt door een overheidsinstantie, (b) de kernactiviteiten bestaan uit regelmatige en systematische monitoring op grote schaal, of (c) de kernactiviteiten bestaan uit grootschalige verwerking van bijzondere categorieën gegevens. De verwerker, als onafhankelijke zelfstandige in dienstverlening aan onderwijsinstellingen, voldoet aan geen van deze criteria: bijzondere-categorie gegevens (doktersattesten) vormen slechts een secundair onderdeel van de dienstverlening en de monitoring betreft enkel de administratieve stageopvolging.

De verwerker heeft wél een **Privacy-contactpunt** ingesteld voor alle AVG-gerelateerde vragen, incidenten, verzoeken van betrokkenen of audits door de verwerkingsverantwoordelijke:

> E-mail: axel@molokini.be
>
> Reactietermijn: binnen 5 werkdagen; urgente datalekken binnen 72 uur conform artikel 33 AVG.

Deze keuze wordt jaarlijks herzien. Bij structurele uitbreiding van de verwerking (bijvoorbeeld nieuwe categorie bijzondere gegevens, substantiële toename van het aantal scholen) kan de aanstelling van een formele DPO alsnog aangewezen zijn.

15. Toezichthoudende autoriteit

Betrokkenen en de verwerkingsverantwoordelijke kunnen een klacht indienen bij:

> **Gegevensbeschermingsautoriteit (GBA)**
>
> Drukpersstraat 35, 1000 Brussel
>
> contact@apd-gba.be — https://www.gegevensbeschermingsautoriteit.be

> **Vlaamse Toezichtcommissie (VTC)**
>
> Bevoegd voor verwerking van persoonsgegevens door Vlaamse onderwijsinstellingen.
>
> https://overheid.vlaanderen.be/vlaamse-toezichtcommissie

16. Slotbepalingen

- Bij tegenstrijdigheid tussen deze DPA en andere overeenkomsten tussen partijen, prevaleert deze DPA voor alle zaken die betrekking hebben op de verwerking van persoonsgegevens, behoudens wat in artikel 13 over de aansprakelijkheidsbeperkingen is bepaald.
- Is een bepaling van deze DPA in strijd met de regelgeving en daardoor nietig of vernietigbaar, dan blijven de overige bepalingen volledig van kracht. Partijen overleggen om die bepaling te vervangen door een bepaling die wel overeenstemt met de regelgeving.
- Op deze DPA is het Belgisch recht van toepassing.
- Geschillen worden beslecht conform de procedure beschreven in de Algemene Voorwaarden; subsidiair zijn de hoven en rechtbanken van het arrondissement Brussel bevoegd, tenzij partijen anders overeenkomen.

17. Ondertekening

Deze DPA wordt als ondertekend beschouwd zodra de verwerkingsverantwoordelijke het Platform in gebruik neemt na acceptatie van de Algemene Voorwaarden. Wenst de school daarnaast een schriftelijk ondertekend exemplaar, dan kan dit document (versie 2.0) via de webpagina van deze DPA als pdf of Word gedownload worden. Beide partijen ondertekenen het, waarna de school het ondertekende exemplaar terugstuurt naar axel@molokini.be.

Opgemaakt te _____ op _____, in twee exemplaren (één per partij), op basis van versie 2.0 van 7 oktober 2026.

De verwerkingsverantwoordelijke	De verwerker
School: _____	**Jacobs, Axel** (h.o. Molokini)
Adres: _____	KBO BE 0896.293.658, Sint-Katharinavest 56, 1500 Halle
Naam ondertekenaar: _____	Naam ondertekenaar: _____
Functie: _____	Functie: _____
Datum: _____	Datum: _____
Handtekening:	Handtekening:

Bijlage 1. Beschrijving van de verwerking

A. Product	Bernadet.: digitaal platform voor het beheer van stagecontracten, urenstaten, kalender en evaluaties in het onderwijs. Aanbieder en verwerker: Jacobs, Axel (h.o. Molokini), Sint-Katharinavest 56, 1500 Halle, België. Productpagina: https://bernadet.be.

Doelgroep en gebruikers	Onderwijsinstellingen met stages. Gebruikers: studenten (mogelijk minderjarig), stagebegeleiders, stagementoren, school- en campusbeheerders, stagegeverbeheerders en vestigingscontactpersonen; ouders of voogden beperkt tot e-mailadres, getypte naam, tijdstip, IP-adres en eventuele opmerking.
B. Onderwerp, duur en aard	Onderwerp: de diensten uit de dienstverleningsovereenkomst. Duur: de duur van die overeenkomst. Aard: het ter beschikking stellen van, en het wijzigen van, gegevens om het Platform te leveren (artikel 3).
C. Doeleinden	Beheer van stagecontracten, urenstaten en stagekalender, evaluaties, digitale handtekeningen, notificaties, PDF-documenten en audit trail (artikel 3). Geen gebruik voor eigen doeleinden van de verwerker, geen reclame en geen profilering.
D. Categorieën persoonsgegevens en bewaartermijnen	Categorieën: zie artikel 4 (identificatie, adres, geboortedatum, opleiding, stage, uren, evaluaties, gezondheidsgegevens als doktersattesten, technische gegevens). Bewaartermijnen: zie artikel 11 en de Privacyverklaring; doktersattesten worden 3 maanden na goedkeuring automatisch verwijderd.
E. Categorieën betrokkenen	Zie artikel 5.
F. Opslag	Applicatie en database: datacenter te Amsterdam (EER). Back-ups: binnen de EER, 7 dagen. Buiten de EER: zie onderdeel G.
G. Subverwerkers en doorgiftegrond	De actuele lijst, met land van verwerking en doorgiftewaarborg, staat in artikel 7 en artikel 8. Doorgiftegronden zijn het EU-US Data Privacy Framework en de Standaardcontractbepalingen (Uitvoeringsbesluit (EU) 2021/914).
H. Gegevensportabiliteit	Exportformaat: JSON (ingebouwde exportfunctie). Overgangsperiode: minstens 30 dagen. Kosten voor de overstap: geen. Werkwijze: de exportfunctie in het Platform; bij problemen via het contactpunt in onderdeel I.
I. Contact	Privacy-contactpunt: axel@molokini.be (zie artikel 14).
J. Versie	2.0, 7 oktober 2026.

Bijlage 2. Melden van datalekken

Bij een inbreuk in verband met persoonsgegevens of een beveiligingsincident met mogelijke gevolgen voor persoonsgegevens deelt de verwerker de onderstaande informatie. Kan niet alles gelijktijdig worden meegedeeld, dan volgt de rest zonder onredelijke vertraging in stappen. De termijnen staan in artikel 10.

- **Kenmerken:** datum en tijdstip van de vaststelling, samenvatting, aard van het incident (lezen, kopiëren, wijzigen, verwijderen of vernietigen, diefstal)
- **Oorzaak** van het incident, voor zover gekend
- **Getroffen betrokkenen** en hun aantal
- **Getroffen gegevens**: soort (met name bijzondere gegevens zoals gezondheidsgegevens, toegangs- en identificatiegegevens, evaluaties) en omvang
- **Waarschijnlijke gevolgen** voor de betrokkenen
- **Maatregelen** om het incident aan te pakken en verdere schade te beperken of te voorkomen
- **Aanspreekpunt** voor meer informatie: axel@molokini.be

Nieuwe maatregelen die uit een incident voortvloeien, worden bij een volgende herziening in bijlage 3 opgenomen.

Bijlage 3. Beveiligingsmaatregelen

Referentiekader is het zekerheidsniveau "Basis" van het Cyber Fundamentals Framework (CCB), zoals uitgewerkt in de lijst "Contractuele vereisten informatieveiligheid en privacy voor EdTech" (Kenniscentrum Digisprong, versie 1.0, 24/02/2026). De verwerker verklaart dat **niet alle maatregelen van die lijst reeds zijn geïmplementeerd**. De tabel hieronder geeft per onderdeel de stand van zaken en, waar nodig, een tijdpad. Ze geldt als contractuele verbintenis. De onderbouwing per maatregel kan op verzoek worden gedeeld met de school, het schoolbestuur of hun functionaris voor gegevensbescherming.

Onderdeel	Stand van zaken	Tijdpad
Inventaris van gegevens, uitbestede diensten en software	Gegevenscategorieën en subverwerkers zijn gedocumenteerd (DPIA, artikel 7). De afhankelijkheden van de applicatie liggen vast in de lock-bestanden (basis voor een software-inventaris, SBOM).	Schriftelijke inventaris van activa en software uiterlijk 31 januari 2027

Onderdeel	Stand van zaken	Tijdpad
Beleid, wetgeving en risicobeheer	DPIA met risicoanalyse en een GDPR-audit zijn uitgevoerd; jaarlijkse herziening is voorzien.	Beknopte informatiebeveiligingsnota die naar deze documenten verwijst: uiterlijk 31 januari 2027
Toegangsbeheer van het Platform	Rolgebaseerde toegang, controle op recordniveau, minimale rechten per rol, scheiding van de gegevens per school. Tweetrapsauthenticatie met een authenticator-app is verplicht voor beheerders en begeleiders.	Reeds geïmplementeerd
Toegang tot de beheeromgeving (hosting, code, e-mail, foutmonitoring)	Toegang tot de server verloopt uitsluitend via SSH met sleutel; aanmelden met wachtwoord is uitgeschakeld. Op de beheeraccounts bij hosting, code, e-mail, foutmonitoring en domeinregistrar is tweetrapsauthenticatie ingeschakeld.	Reeds geïmplementeerd
Netwerk en firewall	Een firewall op de server is actief en laat enkel de poorten voor SSH en webverkeer (HTTP en HTTPS) toe. De database is niet via het netwerk bereikbaar en luistert enkel lokaal op de server.	Reeds geïmplementeerd
Versleuteling	Versleutelde verbindingen (TLS). Bijzondere gegevens (doktersattesten) en geboortedatum zijn versleuteld opgeslagen. Back-ups zijn versleuteld.	Reeds geïmplementeerd
Back-ups en herstel	Dagelijkse versleutelde back-ups binnen de EER (7 dagen), hersteldoelstellingen (RTO 4 uur, RPO 24 uur) en restore-procedure zijn gedocumenteerd. Een onafhankelijke off-site kopie bij een tweede EER-provider ontbreekt nog.	Eerste restore-test uitgevoerd en gelogd uiterlijk 31 januari 2027; off-site back-up gefaseerd, zonder vaste einddatum

Onderdeel	Stand van zaken	Tijdpad
Updates en kwetsbaarheden	Automatische beveiligingsupdates voor het besturingssysteem van de server zijn actief. Overige updates, herstarts en updates van de softwarebibliotheken van het Platform worden niet automatisch doorgevoerd; een vast updateritme en een vaste kwetsbaarheidscontrole zijn nog niet formeel vastgelegd.	Vast updateritme (minstens elk kwartaal, inclusief herstart) en kwetsbaarheidscontrole van de softwarebibliotheken uiterlijk 31 januari 2027
Logging en detectie	Activiteitenlogboek op applicatieniveau, foutmonitoring en gerouleerde serverlogs. Een vast ritme voor het nakijken van serverlogs is nog niet formeel vastgelegd.	Ritme vastleggen uiterlijk 31 januari 2027
Bescherming van de werkplek van de beheerder	Antimalware is actief en wordt up-to-date gehouden op de werkplek van de beheerder. De schijf van de werkplek is versleuteld.	Reeds geïmplementeerd
Incidentrespons en herstel	Melding aan de school binnen 72 uur (artikel 10) en een restore-runbook zijn vastgelegd. Een algemene incidentprocedure met evaluatie achteraf is nog niet apart gedocumenteerd.	Incidentprocedure uiterlijk 31 januari 2027
Ontwikkeling en testen	Wijzigingen worden getest met een geautomatiseerde testsuite op een aparte testdatabase; beveiliging is onderdeel van de ontwikkelpraktijk (beleid, audit en codecontrole).	Reeds geïmplementeerd
Personeel en opleiding	De verwerker is een eenmanszaak: de beheerder is de enige medewerker met toegang en volgt jaarlijks bijscholing rond gegevensbescherming.	Niet van toepassing; bij uitbreiding met medewerkers worden toegangs- en opleidingsmaatregelen aangevuld

Certificeringen of audits door derden: de verwerker beschikt momenteel niet over een certificering. De verwerker kan een gelijkwaardige normering aantonen via bovenstaande documentatie.