Concept-verwerkersovereenkomst (DPA)

SaaS-developer, handelend onder de naam BPV Dashboard, versie 7 oktober 2026

Deze concept-verwerkersovereenkomst (hierna: "Verwerkersovereenkomst") is opgesteld conform artikel 28 van Verordening (EU) 2016/679 (AVG) en is bedoeld om te worden gesloten tussen SaaS-developer, eenmanszaak gevestigd in Bilthoven (KvK 42155608), handelend onder de naam BPV Dashboard ("Verwerker") en de onderwijsinstelling die het BPV Dashboard-platform afneemt ("Verwerkingsverantwoordelijke"). Vul de schoolgegevens in op de daarvoor bestemde plaatsen en neem voor het retourneren van de getekende versie contact op via het demo-/contactformulier op https://bpvdashboard.nl/contact.

Partijen

1. Verwerkingsverantwoordelijke: _____, gevestigd te _____, ingeschreven bij de Kamer van Koophandel onder nummer _____, rechtsgeldig vertegenwoordigd door _____ in de hoedanigheid van _____ (hierna: "Verantwoordelijke").

2. SaaS-developer, eenmanszaak gevestigd in Bilthoven (KvK 42155608), handelend onder de naam BPV Dashboard, vertegenwoordigd door de eigenaar (hierna: "Verwerker").

hierna gezamenlijk te noemen: "Partijen".

Overwegende dat

a. Partijen een hoofdovereenkomst hebben gesloten op grond waarvan Verwerker het BPV Dashboard-platform als onlinedienst levert aan Verantwoordelijke (de "Hoofdovereenkomst");

b. Verwerker in dat kader persoonsgegevens verwerkt ten behoeve van Verantwoordelijke;

c. Partijen op grond van artikel 28 lid 3 AVG verplicht zijn de verwerking schriftelijk vast te leggen.

Artikel 1. Definities

Begrippen in deze Verwerkersovereenkomst hebben de betekenis die de AVG daaraan toekent. Daarnaast geldt:

- "Platform": het BPV Dashboard-platform zoals geleverd op grond van de Hoofdovereenkomst.
- "Betrokkenen": de natuurlijke personen op wie de Persoonsgegevens betrekking hebben.
- "Sub-verwerker": een door Verwerker ingeschakelde derde die in opdracht van Verwerker Persoonsgegevens verwerkt.

Artikel 2. Voorwerp, aard, doel en duur

2.1 Verwerker verwerkt Persoonsgegevens uitsluitend voor het leveren, beheren, ondersteunen en beveiligen van het Platform, en uitsluitend op gedocumenteerde instructie van Verantwoordelijke.

2.2 De aard van de verwerking betreft het hosten, opslaan, ordenen, raadplegen, wijzigen, beveiligen en wissen van Persoonsgegevens in het Platform.

2.3 Het doel van de verwerking is de uitvoering van het BPV-proces van Verantwoordelijke: stagebemiddeling, begeleiding, beoordeling, urenregistratie en verantwoording.

2.4 Deze Verwerkersovereenkomst heeft dezelfde looptijd als de Hoofdovereenkomst.

Artikel 3. Categorieën betrokkenen en persoonsgegevens

3.1 Categorieën betrokkenen: studenten, ouders/verzorgers (uitsluitend voor minderjarigen waar

wettelijk vereist), docenten, BPV-coördinatoren, examinatoren, contactpersonen leerbedrijven, overige medewerkers van Verantwoordelijke.

3.2 Categorieën persoonsgegevens:

- Identificatie- en contactgegevens: naam, geboortedatum, adres, e-mailadres, telefoonnummer, studentnummer.
- Onderwijs- en BPV-gegevens: opleiding, leerjaar, cohort, BPV-overeenkomsten (SOK's), urenregistratie, gespreksverslagen, beoordelingen, voortgangsindicatoren.
- Account- en authenticatiegegevens: gebruikersnaam, gehashte wachtwoorden, geheim voor tweefactorauthenticatie, sessietokens, IP-adres en apparaatgegevens voor registratie.
- BSN: uitsluitend indien Verantwoordelijke daartoe op grond van haar wettelijke taak gerechtigd is en dat in haar instructie heeft vastgelegd.

3.3 Bijzondere categorieën persoonsgegevens worden in beginsel niet verwerkt. Mocht Verantwoordelijke onverhoopt dergelijke gegevens (bijvoorbeeld gezondheidsgegevens in een gespreksverslag) invoeren, dan geschiedt dit onder uitsluitende verantwoordelijkheid van Verantwoordelijke.

Artikel 4. Verplichtingen Verwerker

4.1 Verwerker verwerkt Persoonsgegevens uitsluitend op gedocumenteerde instructie van Verantwoordelijke. Deze Verwerkersovereenkomst, de Hoofdovereenkomst en redelijke wijzigingsinstructies van Verantwoordelijke kwalificeren als zodanig.

4.2 Verwerker informeert Verantwoordelijke onverwijld indien een instructie naar zijn mening in strijd is met de AVG of andere toepasselijke wetgeving.

4.3 Verwerker waarborgt dat de personen die zij machtigt om Persoonsgegevens te verwerken, een geheimhoudingsplicht hebben aanvaard of door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden.

4.4 Verwerker verleent Verantwoordelijke, rekening houdend met de aard van de verwerking, redelijke bijstand bij het voldoen aan haar verplichtingen onder de artikelen 32 tot en met 36 AVG (beveiliging, datalekken, DPIA en voorafgaande raadpleging).

Artikel 5. Beveiliging (artikel 32 AVG)

5.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze maatregelen omvatten ten minste:

- Versleuteling van gevoelige velden en uploads met AES-256-GCM; sleutelbeheer gescheiden van de database; rouleerbare sleutels.
- Versleuteling van gegevens tijdens overdracht met TLS 1.2 of hoger; HSTS afgedwongen.
- Verplichte tweefactorauthenticatie voor medewerkers van Verantwoordelijke en voor beheerders van Verwerker.
- Rolgebaseerde autorisatie met alleen de minimaal benodigde rechten; een volledig auditlog van inlogpogingen, tweefactorauthenticatie, rolwisselingen, wachtwoordherstel en uitloggen.
- Beveiligingsheaders (CSP, HSTS, X-Frame-Options en Permissions-Policy) en beperkingen op het aantal verzoeken bij authenticatie.
- Periodieke versleutelde back-ups; periodieke hersteltests.
- Periodieke kwetsbaarheidsscans en, ten minste jaarlijks, een externe penetratietest.
- Gedocumenteerde procedures voor incident- en wijzigingsbeheer.

5.2 Verwerker evalueert deze maatregelen periodiek en past ze aan op basis van de stand der techniek en het actuele risicoprofiel. Het beveiligingsniveau blijft te allen tijde minimaal gelijkwaardig aan het in

dit artikel beschreven niveau.

Artikel 6. Subverwerkers (artikel 28 lid 2 en 4 AVG)

6.1 Verantwoordelijke verleent Verwerker algemene toestemming voor het inschakelen van Sub-verwerkers. De actuele lijst van Sub-verwerkers is opgenomen in Bijlage 2 en wordt door Verwerker actueel gehouden.

6.2 Verwerker informeert Verantwoordelijke ten minste 30 dagen vooraf over voorgenomen wijzigingen in de Sub-verwerkers. Verantwoordelijke kan binnen die termijn gemotiveerd bezwaar maken. Komen Partijen er niet uit, dan heeft Verantwoordelijke het recht de Hoofdovereenkomst kosteloos op te zeggen tegen de ingangsdatum van de wijziging.

6.3 Verwerker legt aan iedere Sub-verwerker schriftelijk verplichtingen op die ten minste gelijkwaardig zijn aan die in deze Verwerkersovereenkomst.

6.4 Het BPV Dashboard-platform draait op Microsoft Azure. De applicatie en database worden gehost binnen de EU (Zweden). Persoonsgegevens worden versleuteld opgeslagen.

Artikel 7. Doorgifte buiten de EER

7.1 Doorgifte naar een derde land of internationale organisatie buiten de EER vindt uitsluitend plaats indien dit is toegestaan op grond van hoofdstuk V AVG (adequaatheidsbesluit of passende waarborgen zoals standaardcontractbepalingen, voorzien van aanvullende maatregelen waar nodig) en Verantwoordelijke daarvan vooraf in kennis is gesteld.

Artikel 8. Verzoeken van Betrokkenen

8.1 Verwerker verleent Verantwoordelijke, rekening houdend met de aard van de verwerking, redelijke bijstand door middel van passende technische en organisatorische maatregelen om te voldoen aan haar plicht om verzoeken van Betrokkenen tot uitoefening van hun rechten (artikelen 12 tot en met 23 AVG) af te handelen.

8.2 Verwerker stuurt verzoeken die rechtstreeks bij haar binnenkomen, onverwijld door naar Verantwoordelijke en beantwoordt deze niet zelfstandig.

Artikel 9. Datalekken (artikelen 33 en 34 AVG)

9.1 Verwerker meldt iedere inbreuk in verband met Persoonsgegevens (datalek) onverwijld en uiterlijk binnen 24 uur na ontdekking aan de Functionaris voor Gegevensbescherming of vaste contactpersoon van Verantwoordelijke.

9.2 De melding bevat in ieder geval de aard van het datalek, de (geschatte) categorieën en aantallen Betrokkenen en datarecords, de waarschijnlijke gevolgen, de getroffen en voorgestelde maatregelen, en de contactgegevens van de FG of contactpersoon van Verwerker.

9.3 De melding aan de Autoriteit Persoonsgegevens en, indien vereist, aan de Betrokkenen geschiedt door Verantwoordelijke. Verwerker verleent daarbij alle redelijke medewerking.

9.4 Verwerker houdt een intern datalekregister bij en stelt dit op verzoek aan Verantwoordelijke en de FG ter inzage.

Artikel 10. Controle (artikel 28 lid 3 sub h AVG)

10.1 Verwerker stelt aan Verantwoordelijke alle informatie ter beschikking die nodig is om de naleving van de in dit artikel en artikel 28 AVG neergelegde verplichtingen aan te tonen.

10.2 Verwerker maakt controles, waaronder inspecties, door Verantwoordelijke of een door Verantwoordelijke gemachtigde controleur mogelijk en draagt eraan bij. Controles vinden maximaal

eenmaal per kalenderjaar plaats, tenzij er een concrete aanleiding is, en worden minimaal 30 dagen tevoren schriftelijk aangekondigd.

10.3 Verwerker mag verlangen dat de controleur een geheimhoudingsverklaring tekent. Indien Verwerker beschikt over een actuele assuranceverklaring (bijvoorbeeld ISO 27001 of SOC 2 Type II) ten aanzien van de Dienst, kan Verantwoordelijke instemmen om deze als bewijs van naleving te aanvaarden.

10.4 De kosten van een controle komen voor rekening van Verantwoordelijke, tenzij uit de controle blijkt dat Verwerker tekortschiet in de nakoming van deze Verwerkersovereenkomst.

Artikel 11. Aansprakelijkheid en boetes

11.1 De aansprakelijkheid van Partijen wordt beheerst door de Hoofdovereenkomst, voor zover en zoals daarin overeengekomen, met inachtneming van de dwingendrechtelijke bepalingen van artikel 82 AVG.

11.2 Een eventueel door de Autoriteit Persoonsgegevens aan een Partij opgelegde bestuurlijke boete komt voor rekening van de Partij aan wie de overtreding kan worden toegerekend. Boetes worden niet gezien als directe of indirecte schade in de zin van de Hoofdovereenkomst.

Artikel 12. Einde van de verwerking

12.1 Bij beëindiging van de Hoofdovereenkomst, ongeacht de reden, stelt Verwerker, naar keuze van Verantwoordelijke, alle Persoonsgegevens binnen 30 dagen ter beschikking aan Verantwoordelijke in een gangbaar, gestructureerd machine-leesbaar formaat, dan wel vernietigt Verwerker deze.

12.2 Na de overeengekomen exporttermijn vernietigt Verwerker de Persoonsgegevens (inclusief kopieën en logbestanden waarin deze voorkomen) binnen 60 dagen, behoudens wettelijke bewaarverplichtingen. Op verzoek verstrekt Verwerker een schriftelijke vernietigingsverklaring.

Artikel 13. Slotbepalingen

13.1 Bij tegenstrijdigheid tussen deze Verwerkersovereenkomst en de Hoofdovereenkomst prevaleert deze Verwerkersovereenkomst voor zover het de verwerking van Persoonsgegevens betreft.

13.2 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement van de statutaire vestigingsplaats van Verwerker.

13.3 Wijzigingen van deze Verwerkersovereenkomst zijn slechts geldig indien schriftelijk overeengekomen en door beide Partijen ondertekend.

Ondertekening

Namens Verantwoordelijke

Naam: _____

Functie: _____

Plaats: _____

Datum: _____

Handtekening:

Namens Verwerker (SaaS-developer)

Naam: _____

Functie: _____

Plaats: _____

Datum: _____

Handtekening:

Bijlage 1. Specificatie van de verwerking

- Onderwerp: het verwerken van Persoonsgegevens ten behoeve van de uitvoering van het BPV-proces in het Platform.
- Aard en doel: zoals beschreven in artikel 2.
- Categorieën Betrokkenen en Persoonsgegevens: zoals beschreven in artikel 3.
- Duur: gelijk aan de looptijd van de Hoofdovereenkomst, vermeerderd met de termijnen voor export en vernietiging uit artikel 12.
- Bewaartermijnen: conform de door Verantwoordelijke vastgestelde termijnen, gebaseerd op de WEB, het Uitvoeringsbesluit WEB en het eigen bewaarbeleid; standaard 7 jaar voor BPV-dossiers na uitstroom, tenzij Verantwoordelijke schriftelijk anders instrueert.

Bijlage 2. Subverwerkers (peildatum 7 oktober 2026)

- Microsoft Azure: hosting van applicatie, database en back-ups binnen de EU (Zweden).
- Resend: transactionele e-mail voor wachtwoordherstel, meldingen en exports.
- Aanbieder van webpush: bezorging van pushmeldingen.
- OpenStreetMap Nominatim: geocodering (openbare dienst; verwerkt uitsluitend adresgegevens van leerbedrijven; geen DPA vereist).

Bijlage 3. Beveiligingsmaatregelen (samenvatting)

- Versleutelde opslag: AES-256-GCM voor gevoelige velden en uploads; vervangbaar sleutelbeheer.
- Versleutelde overdracht: TLS 1.2 of hoger, HSTS en moderne versleutelingsmethoden.
- Authenticatie: verplichte tweefactorauthenticatie voor alle accounts van medewerkers; sterk wachtwoordbeleid; optie om een vertrouwd apparaat maximaal 7 dagen te onthouden.
- Autorisatie: rolgebaseerde toegang, alleen de minimaal benodigde rechten en tijdelijke toegang voor beheerders.
- Registratie: volledig auditlog van inloggen, tweefactorauthenticatie, rolwisselingen, wachtwoordherstel en uitloggen; bewaartermijn 24 maanden.
- Netwerk: WAF en beperkingen op het aantal verzoeken (inloggen 10 per 15 minuten, tweefactorauthenticatie 5 per 15 minuten, wachtwoordherstel 5 per uur en openbare formulieren 15 per uur).
- Headers: CSP, HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.
- Back-up: dagelijkse versleutelde back-ups en periodieke hersteltests.
- Personeel: geheimhoudingsverklaring, screening, AVG-training en beleid voor een opgeruimde werkplek en vergrendelde schermen.
- Toetsing: jaarlijkse externe penetratietest; ISO 27001-traject in voorbereiding.