

20 mei 2025

Rapportagemodel DPIA Rijksdienst - CEM

MBO Raad

Versie 1.0

Voor MBO Raad

Door ICTRecht



Inhoudsopgave

1. Managementsamenvatting	3
2. Overzicht risico's en acties	4
3. Beschrijving kenmerken gegevensverwerking	10
3.1 Voorstel	10
3.2 Persoonsgegevens	14
3.3 Gegevensverwerkingen	18
3.4 Technieken en methoden van de gegevensverwerkingen	19
3.5 Verwerkingsdoeleinden	20
3.6 Betrokken partijen	21
3.7 Belangen bij de gegevensverwerkingen	23
3.8 Verwerkingslocaties	24
3.9 Juridisch en beleidsmatig kader	25
3.10 Bewaartermijnen	26
4. Beoordeling rechtmatigheid gegevensverwerkingen	28
4.1 Rechtsgrond	28
4.2 Bijzondere persoonsgegevens	29
4.3 Doelbinding	29
4.4 Noodzaak en evenredigheid	32
4.5 Rechten van betrokkenen	34
5. Beschrijving en beoordeling risico's voor betrokkenen	36
6. Maatregelen en restrisico's	41
7. Ondertekening	46

1. Managementsamenvatting

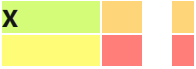
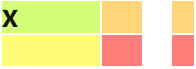
MBO Raad is een brancheorganisatie van alle Rijksbekostigde mbo-instellingen in Nederland. MBO Digitaal (onderdeel van MBO Raad) heeft ons, ICTRecht B.V. ('ICTRecht'), gevraagd om een centrale *Data Protection Impact Assessment* ('DPIA') uit te voeren ten aanzien van de verwerkingen van persoonsgegevens door de Coöperatie Examens MBO ('CEM') in haar rol als verwerker ten opzichte van de mbo-instellingen.

De CEM is een coöperatie welke digitale (reken)examens, en andere acties die op deze processen zijn gestoeld, levert aan bijna alle mbo-instellingen in Nederland. Er worden veel persoonsgegevens verwerkt door de CEM. Aangezien het gaat om een grootschalige verwerking van persoonsgegevens en gegevens met betrekking tot kwetsbare betrokkenen, is een DPIA verplicht. Aan de hand van een DPIA doet een organisatie voorafgaand onderzoek naar de privacyrisico's die spelen bij een bepaalde gegevensverwerking. Het is de bedoeling om de risico's in kaart te brengen en maatregelen te bedenken waarmee de risico's uiteindelijk verkleind kunnen worden.

De DPIA is, zoals wettelijk verplicht, uitgevoerd vanuit het oogpunt van de verwerkingsverantwoordelijke (mbo-instelling). Dat betekent dat er in deze DPIA risico's zijn geconstateerd ten aanzien van de mbo-instelling als verwerkingsverantwoordelijke, maar ook ten aanzien van de CEM als verwerker en ten opzichte van haar leveranciers als subverwerkers. Een overzicht van de risico's en voorgestelde acties is opgenomen in het volgende hoofdstuk.

2. Overzicht risico's en acties

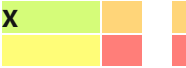
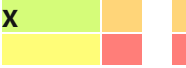
Hieronder volgen de geconstateerde risico's en voorgestelde maatregelen om deze risico's te mitigeren.

	Risico	Acties	Beheer der acties	Risicobeoordeling	
1	Het risico bestaat dat het overzicht van verwerkte persoonsgegevens (het verwerkingsregister) binnen de mbo-instelling niet up-to-date is. Dit kan leiden tot situaties waarin betrokkenen hun rechten niet kunnen uitoefenen, en tot het niet voldoen aan de verantwoordingsplicht die op mbo-instellingen als verwerkingsverantwoordelijke rust.	Mbo-instellingen dienen het verwerkingsregister bij te werken met alle verwerkingen die worden uitgevoerd door de CEM. Daarbij dient onder andere te worden uitgelegd welke persoonsgegevens worden verwerkt, hoelang de gegevens bewaard blijven en welke beveiligingsmaatregelen zijn getroffen.	Mbo-instellingen	Kans X Schade Na het treffen van maatregelen is het restryisiko laag.	
2	De CEM beschikt op dit moment niet over een verwerkingsregister waarin de verwerkingen, die worden uitgevoerd in de hoedanigheid van verwerker, zijn opgenomen. Dit kan leiden tot een gebrek aan inzicht in verwerkingen die worden uitgevoerd ten behoeve van de mbo-instellingen en verhoogde risico's op onrechtmatige of onveilige gegevensverwerking.	De CEM stelt zo spoedig mogelijk een volledig en actueel verwerkingsregister op waarin alle verwerkingen zijn opgenomen die namens de mbo-instellingen worden uitgevoerd in de hoedanigheid van verwerker. Dit register voldoet aan de eisen uit artikel 30 AVG en bevat ten minste: • de doeleinden van de verwerkingen; • een beschrijving van de categorieën van betrokkenen en persoonsgegevens; • de categorieën van ontvangers;	CEM	Kans X Schade Na het treffen van maatregelen is het restryisiko laag.	

- eventuele doorgiften aan derde landen;
- beoogde termijnen voor het wissen van gegevens;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

3	Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen door CEM niet vooraf door mbo-instellingen zelf zijn vastgelegd, eveneens in het verwerkingsregister. Dat zou leiden tot een onrechtmatige verwerking die ook de uitoefening door betrokkenen van hun rechten kan belemmeren.	Mbo-instellingen dienen zelf de verwerkingsdoeleinden vast te stellen en vast te leggen in het verwerkingsregister. Enkel benoeming van de (algemene) verwerkingsdoeleinden in deze DPIA volstaat niet voor het voldoen aan de verantwoordingsplicht.	Mbo-instellingen	Kans X Schade Na het treffen van maatregelen is het restryrisico laag.
4	Binnen beide gegevensverwerkingen (het plannen/vaststellen en het afnemen/analyseren van examens) worden persoonsgegevens verwerkt die niet strikt noodzakelijk zijn voor het bereiken van het verwerkingsdoel. Het betreft hier onder meer de adresgegevens (adres, plaats, postcode, land) van medewerkers en studenten, alsook gezondheidsgegevens van studenten (zoals informatie over extra tijd of visuele	Paragin dient een gegevensreductie door te voeren. Verwerken enkel de strikt noodzakelijke gegevens. Schakel de optionele velden (zoals adresgegevens) standaard uit tenzij expliciet gemotiveerd.	Paragin	Kans X Schade Na het treffen van maatregelen is het restryrisico laag.

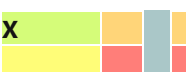
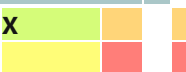
beperkingen).
Verwerking van niet-noodzakelijke persoonsgegevens leidt tot een schending van het beginsel van dataminimalisatie zoals voorgeschreven door de AVG. Dit verhoogt het risico op datalekken en ongeoorloofde toegang tot gevoelige informatie, met mogelijke reputatieschade en juridische gevolgen voor de mbo-instelling.

5	Het risico bestaat dat persoonsgegevens langer worden bewaard dan noodzakelijk. Dat risico kan ontstaan doordat ofwel geen bewaartermijn is vastgesteld ofwel doordat bewaartermijnen niet consequent worden gehandhaafd. Dat leidt tot een onrechtmatige verwerking van persoonsgegevens en tot een groter risico bij beveiligingsincidenten.	De mbo-instelling dient de bewaartermijnen vast te stellen en vast te leggen. De mbo-instelling is zelf verantwoordelijk voor (geautomatiseerde) verwijdering. Wij adviseren de mbo-instellingen om geautomatiseerde verwijdering van reeds vastgestelde termijnen in te voeren. Paragin dient de opschoontermijn die standaard staat ingesteld op 'nooit' aan te passen, zodat de persoonsgegevens niet langer standaard oneindig bewaard worden.	Mbo-instellingen en Paragin	Kans X  Schade Na het treffen van maatregelen is het restrisico laag.
6	Het risico bestaat dat er geen passende afspraken zijn gemaakt met partijen door wie persoonsgegevens worden verwerkt. Als dit niet, niet tijdig, of niet correct wordt gedaan, ontstaat het	De mbo-instelling dient een verwerkersovereenkomst te sluiten met de CEM. De CEM dient daarnaast nog een verwerkersovereenkomst te sluiten met leverancier Stipp.	Mbo-instellingen en CEM	Kans X  Schade Na het treffen van maatregelen is het restrisico laag.

risico dat de ontvangende partij de persoonsgegevens onbehoorlijk verwerkt. Dit leidt voor betrokkenen tot het risico op misbruik van persoonsgegevens, datalekken, verlies van vertrouwelijkheid, en dat betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen.

7	Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op de mbo-instellingen rust. Hierdoor kunnen betrokkenen niet verwachten en/of anticiperen op welke wijze de desbetreffende partijen met hun persoonsgegevens omgaan. Dit leidt ertoe dat betrokkenen hun rechten niet of minder goed kunnen uitoefenen.	De mbo-instelling dient betrokkenen te informeren over de verwerking van hun persoonsgegevens. Dit dient zij te doen door middel van de privacyverklaring voor studenten en door middel van de privacyverklaring voor medewerkers.	Mbo-instellingen	Kans X Schade Na het treffen van maatregelen is het restrisico laag.
8	Het risico bestaat dat persoonsgegevens bij CEM ongeautoriseerd toegankelijk zijn, doordat geen encryptie wordt toegepast op data-at-rest en data-in-transit. Hoewel op onderdelen gegevens worden geanonimiseerd, zijn andere gegevens onvoldoende beschermd bij een beveiligingsincident.	De CEM dient persoonsgegevens te beveiligen door versleuteling toe te passen op data-at-rest en data-in-transit. Dit dient zij te doen door het implementeren van encryptietechnieken conform actuele beveiligingsstandaarden (zoals AES-256 en TLS 1.2 of hoger) in alle systemen waarin persoonsgegevens	CEM	Kans X Schade Na het treffen van maatregelen is het restrisico laag.

Dit kan ertoe leiden dat persoonsgegevens van betrokkenen bij verlies of diefstal van gegevens ongewenst worden ingezien, wat schade kan veroorzaken aan hun privacy.

9	Het risico bestaat dat incidenten en afwijkingen in de verwerking van persoonsgegevens niet tijdig worden gedetecteerd, aangezien CEM geen gebruikmaakt van actieve monitoring of geautomatiseerde detectiesystemen. In de praktijk worden afwijkingen vooral opgemerkt via meldingen aan de supportdesk. Hierdoor is de kans aanwezig dat onregelmatigheden pas laat aan het licht komen, waardoor betrokkenen gedurende langere tijd risico lopen op verlies van BIV van hun persoonsgegevens, zonder dat zij hiervan op de hoogte worden gesteld of bescherming kunnen inroepen.	De CEM dient incidenten en afwijkingen in de verwerking van persoonsgegevens tijdig te detecteren. Dit dient zij te doen door middel van actieve monitoring en het inzetten van geautomatiseerde detectiesystemen voor het signaleren van onregelmatigheden in gegevensverwerkingen.	CEM	Kans  Schade Na het treffen van maatregelen is het restryrisico laag.
10	Het risico bestaat dat beveiligingsrisico's en kwetsbaarheden binnen CEM onvoldoende tijdig of volledig in beeld zijn, aangezien er geen structureel risicomanagementproces is ingericht. Risico-identificatie	De CEM dient beveiligingsrisico's en kwetsbaarheden structureel in kaart te brengen. Dit dient zij te doen door middel van het inrichten en uitvoeren van een risicomanagementproces dat periodiek risico's identificeert, beoordeelt	CEM	Kans  Schade Na het treffen van maatregelen is het restryrisico laag.

vindt vooral plaats op incidentele basis of wanneer er concrete aanleiding toe is. Hierdoor bestaat het risico dat bestaande dreigingen en zwakke plekken in systemen of processen onopgemerkt blijven, met als gevolg dat persoonsgegevens van betrokkenen in onvoldoende beveiligde omgevingen worden verwerkt.

1	Het risico bestaat dat binnen Paragin medewerkers toegang hebben tot persoonsgegevens zonder dat dit noodzakelijk is voor de uitvoering van hun functie. Hoewel Paragin aangeeft passende beheersmaatregelen te hebben getroffen, is niet vastgesteld dat toegang tot persoonsgegevens strikt is ingericht op basis van rollen en 'need-to-know'. Dit verhoogt het risico dat persoonsgegevens van betrokkenen worden ingezien of verwerkt door onbevoegde medewerkers, wat kan leiden tot verlies van vertrouwelijkheid en een beperking van de controle die betrokkenen over hun gegevens hebben.	Paragin dient de toegang tot persoonsgegevens te beperken tot medewerkers voor wie dit noodzakelijk is. Dit dient zij te doen door middel van een strikt rol gebaseerd toegangsbeheer op basis van het 'need-to-know'-principe en door periodiek te controleren of de toegangsrechten aansluiten bij de functieverantwoordelijkheden.	Paragin	Kans X			
1					Schade		
					Na het treffen van maatregelen is het restrisico laag.		

3. Beschrijving kenmerken gegevensverwerking

In dit hoofdstuk volgt een beschrijving van de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen. Hieronder wordt een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen geboden, op welke informatie het resterende deel van de DPIA is gebaseerd.

3.1 Voorstel

Deze paragraaf beschrijft het voorstel waar de DPIA op toeziet op hoofdlijnen.

MBO Raad is een brancheorganisatie van alle Rijksbekostigde mbo-instellingen in Nederland. MBO Digitaal (onderdeel van MBO Raad) heeft ons, ICTRecht B.V. ('ICTRecht'), gevraagd om een centrale *Data Protection Impact Assessment* ('DPIA') uit te voeren ten aanzien van de verwerkingen van persoonsgegevens door de Coöperatie Examens MBO ('CEM') in haar rol als verwerker ten opzichte van de mbo-instellingen. De DPIA is, zoals wettelijk verplicht, uitgevoerd door de verwerkingsverantwoordelijke (mbo-instelling). Dat betekent dat er in deze DPIA risico's zijn geconstateerd ten aanzien van de mbo-instelling als verwerkingsverantwoordelijke, maar ook ten aanzien van de CEM als verwerker en ten opzichte van haar leveranciers als subverwerkers.

De CEM is een coöperatie welke, aan bijna alle scholen in het middelbaar beroepsonderwijs ('mbo') in Nederland, digitale (reken)examens, en andere acties die op deze processen zijn gestoeld, levert.

De CEM verwerkt veel persoonsgegevens. Aangezien het gaat om een grootschalige verwerking van persoonsgegevens en gegevens met betrekking tot kwetsbare betrokkenen, is een DPIA verplicht.¹ De verwerking is op basis van criteria gegeven door de Autoriteit Persoonsgegevens grootschalig, vanwege het grote aantal betrokkenen (ongeveer 250.000 studenten en 400 beoordelaars per jaar), de grote hoeveelheid gegevens die mogelijk worden verwerkt (NAW-gegevens, examenresultaten, gezondheidsgegevens etc.), de duur van de verwerking (afhankelijk van de door de mbo-instelling ingestelde bewaartermijn) en de geografische reikwijdte van de verwerking (betrokkenen door heel Nederland). Daarnaast hebben de gegevens (deels) betrekking op kwetsbare betrokkenen, namelijk minderjarige mbo-scholieren.

Aan de hand van een DPIA doet een organisatie voorafgaand onderzoek naar de privacyrisico's die spelen bij een bepaalde gegevensverwerking. Het is de bedoeling om de risico's in kaart te brengen en maatregelen te bedenken waarmee de risico's uiteindelijk verkleind kunnen worden.

In deze DPIA worden de verwerkingen van persoonsgegevens door de CEM in haar rol als verwerker ten behoeve van de mbo-instellingen getoetst aan de Algemene

¹ Artikel 29-Werkgroep, WP 248 rev.01 'richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679', 4 oktober 2017.

verordening gegevensbescherming² ('AVG') en de Uitvoeringswet AVG³ ('UAVG'). Aanvullend is rekening gehouden met de richtlijn van het Europees Comité voor gegevensbescherming (voorheen: Artikel 29-Werkgroep) inzake het uitvoeren van een DPIA.⁴

Hoewel informatiebeveiliging geen expliciet onderdeel vormt van het Rijksmodel DPIA, is dit thema wel degelijk van essentieel belang voor een zorgvuldige beoordeling van de gegevensverwerkingen. In het kader van deze DPIA zijn gesprekken gevoerd met alle (sub)verwerkers, waaronder CEM en Paragin, om inzicht te verkrijgen in de wijze waarop zij de beveiliging van hun systemen hebben ingericht. De uitkomsten van deze gesprekken zijn vertaald naar concrete risico's op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens, zoals bedoeld in artikel 32 AVG. Deze risico's zijn opgenomen in de risicoanalyse in hoofdstuk 4 en voorzien van passende mitigerende maatregelen in hoofdstuk 5.

Als input zijn verschillende documenten geraadpleegd en hebben er verschillende overleggen plaatsgevonden tussen stakeholders, waaronder de CEM, Cito, Paragin, Stipp en ICTRecht.

In deze DPIA zal een onderscheid gemaakt worden tussen verschillende gegevensverwerkingen die de CEM uitvoert in haar rol als verwerker, ten behoeve van de mbo-instellingen. Daarbij wordt een onderscheid gemaakt tussen verschillende onderdelen die samen het gehele proces rondom de digitale (reken)examens vormen. Het gehele proces rondom de digitale (reken)examens is onder te verdelen in zeven onderdelen:

1. Examenmatrijs, constructie en normering
2. Vaststelling examen
3. Afname examen
4. Beoordelen, verwerken en analyse
5. Registreren en communiceren
6. Vaststellen, communiceren, resultaten en inzage
7. Evalueren en verbeteren

De onderdelen examenmatrijs en constructie (1), afname examen (3), beoordelen, verwerken en analyse (4), registreren en communiceren (5), vaststellen, communiceren, resultaten en inzage (6) en evalueren en verbeteren (7) vinden (deels) plaats in Remindo, de online examenomgeving van leverancier Paragin. Alle deelnemende mbo-instellingen hebben een eigen besloten examenomgeving om examens vast te stellen en in te plannen (2), af te nemen (3) en eventueel te

² Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (AVG).

³ Wet van 16 mei 2018, houdende regels ter uitvoering van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming) (pbeu 2016, I 119) (UAVG).

⁴ Artikel 29-Werkgroep, WP 248 rev.01 'richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679', 4 oktober 2017.

beoordelen (4). Daarnaast levert Paragin voor de Entree-opleiding⁵, MijnRekenPortfolio/Skillsly voor de metingen van het rekenen. Bij het onderdeel normering (1), analyse (4) en evalueren en verbeteren (7) werkt de CEM samen met de psychometrische afdeling van het Centraal Instituut voor Toetsontwikkeling ('CITO'). Voor het inplannen van beoordelaars voor de (reken)examens gebruikt de CEM de Beoordelaarsmodule van leverancier Stipp.

Overige koppelingen vallen buiten de scope van deze DPIA, zoals de beveiligingssoftware (o.a. 'Schoolyear'), plansoftware (o.a. 'OnTrac')⁶, schooleigen software en de verklankingssoftware geïntegreerd in Remindo ('Readspeaker').

Remindo en MijnRekenPortfolio/Skillsly (Paragin)

De (reken)examens op niveau MBO 2, 3 en 4 worden ontwikkeld en afgenomen middels het digitaal examenplatform Remindo. De afname van de (reken)examens en de metingen vinden plaats onder verantwoording van de mbo-instellingen. De afname omgevingen voor de toetsen zijn gescheiden per mbo-instelling. Deze besloten omgeving is toegankelijk via de schooleigen Remindo-omgeving. Andere mbo-instellingen hebben hier geen toegang tot. In deze eigen besloten examenomgeving kan de mbo-instelling zelf (reken)examens vaststellen, inplannen (en koppelen aan kandidaten), afnemen en (eventueel) beoordelen. Alleen medewerkers (zie rollen hieronder) van de mbo-instelling krijgen toegang tot de eigen examenomgeving in Remindo. De CEM levert vanuit de centrale beheeromgeving het (reken)examen aan de mbo-instelling en na de vaststelling van het (reken)examen kan de mbo-instelling het (reken)examen plannen en afnemen.

In de digitale afname-omgeving bestaan diverse rollen, zoals IT-beheerder, beheerder, vaststelling-/examencommissie, beoordelaar, rekendocent, entree-rekendocent, entree beheerder, surveillant en student. Studenten krijgen uitsluitend via hun mbo-instelling toegang tot Remindo gedurende de tijdsduur van het (oefen-)examen en de periode daarvoor om kandidaat informatie te lezen. De CEM of Paragin kan, in geval van nood of na toestemming van de mbo-instelling, in de digitale omgeving van de desbetreffende mbo-instelling. De CEM en Paragin kunnen via het logboek zien wie het (reken)examen voor het laatst heeft aangepast en goedgekeurd.

De gegevens van studenten (account en examenresultaten) in deze digitale examenomgeving worden uitsluitend door de mbo-instelling zelf beheerd. Het systeem is zo ingericht dat herleidbare persoonsgegevens uitsluitend binnen de digitale beveiligde omgeving van de mbo-instelling wordt verwerkt. Studentgegevens komen geautomatiseerd in de afnameomgeving of MijnRekenPortfolio/Skillsly door koppelvlakken ('OO API') met het Studentinformatiesysteem ('SIS')/Leerling Administratie Systeem ('LAS') of via een Excel import. De behaalde scores gaan vervolgens via Remindo weer terug naar het SIS.

De IT-beheerder van de mbo-instelling is verantwoordelijk voor de koppelingen met het SIS/LAS, beveiligingsinstellingen en het archiveren/verwijderen van examenresultaten. Zo kunnen mbo-instellingen in Remindo zelf ervoor kiezen om gegevens van medewerkers of studenten geautomatiseerd te anonimiseren na X aantal jaar en/of randomisatie waarin een bepaald percentage van de resultaten wordt toegewezen aan een andere groep. Ook kan de mbo-instelling per rol

⁵ De entree-opleiding is een Mbo-niveau 1 opleiding. Voor de entreeopleiding is geen diploma vereist van een vooropleiding.

⁶ Ten aanzien van OnTrac is eerder een DPIA uitgevoerd door ICTRecht in opdracht van de MBO Raad.

(kandidaat, begeleider, beheerder, etc.) aangeven welke persoonsgegevens vereist zijn om in te vullen.

Remindo maakt het daarnaast mogelijk dat medewerkers en studenten met hun eigen instellingsaccount kunnen inloggen. Hierdoor hoeven scholen geen aparte gebruikersaccounts meer aan te maken, maar kunnen bestaande accountgegevens (her)gebruikt worden. Wel kan een mbo-instelling ervoor kiezen om met gebruikersnaam en wachtwoord in te moeten loggen, in plaats van met het instellingsaccount via SSO ('Single Sign On'). In Remindo staan niet alleen gegevens die nodig zijn voor de identificatie van de studenten, maar ook gezondheidsgegevens met betrekking tot extra tijd voor bijvoorbeeld blinden of slechtzienden.

Remindo bestaat uit twee omgevingen. Enerzijds een auteursomgeving waarmee de CEM, de constructeurs, vaststellers en analisten werken en anderzijds de afname omgeving: het gedeelte waarmee de mbo-instellingen werken. Dit is voor het beheren, vaststellen, plannen, afnemen, surveilleren, (eventueel) beoordelen en het maken van analyses.

Psychometrische analyse (Cito)

Bij het onderdeel normering (1), analyse (4) en evalueren en verbeteren (7) werkt de CEM samen met de psychometrische afdeling van Cito. Het CitoLab van Cito voert onderzoek en analyses uit op de afgenomen (reken)examens. Deze (reken)examens staan voor een bepaalde tijd open en daarna volgt de normering.

De CEM kan via haar eigen portal in Remindo en de beoordelaarsmodule van Stipp alle (reken)examen gerelateerde informatie ophalen. Dit betreft anonieme data voor kwaliteitsdoeleinden, zoals de psychometrische evaluatie van (reken)examens. Door analyses uit te voeren, kan het Cito de normering van de (reken)examens bepalen. De benodigde data worden via een API uit Remindo gehaald en vervolgens in een Excel-tabel verwerkt.

Bij de kandidaat worden twee kenmerken vastgelegd: een session ID (een geanonimiseerd nummer) om responses te koppelen aan een specifieke kandidaat, en een user ID (willekeurig gegenereerd) voor gevallen waarin een student een (reken)examen aflegt en later opnieuw deelneemt. Daarnaast wordt geregistreerd bij welke mbo-instelling het (reken)examen is afgenomen, om welke toets het gaat en wat de behaalde score is.

Beoordelaarsmodule (Stipp)

Voor het inplannen van beoordelaars van de (reken)examens gebruikt de CEM de Beoordelaarsmodule van Stipp. Stipp werkt voor het realiseren hiervan samen met Paragin. Vanuit de Beoordelaarsmodule worden beoordelaars toegewezen om (reken)examens van een student van een andere mbo-instelling te beoordelen. Iedere mbo-instelling levert namelijk capaciteit voor het beoordelen van de open vragen in de (reken)examens. De CEM levert de lijst met beoordelaars aan Stipp.

De Beoordelaarsmodule zit tussen Remindo en de beoordelaars in. Gemaakt werk wordt anoniem en geautomatiseerd gekoppeld aan twee beoordelaars. De Beoordelaarsmodule van Stipp heeft een koppeling met Remindo. Voor de beoordeling zelf worden de beoordelaars doorgezet naar Remindo. Ook vinden steekproeven en controles plaats of er afwijkingen in de beoordeling zitten. Verder verzamelt Stipp statistieken over de planning en voortgang van de (reken)examens via een dashboard. Stipp logt alles wat ze van Remindo binnenkrijgen. Deze logging bevat persoonsgegevens.

Stipp ontvangt van de studenten onder andere de kandidaat ID's, testmoment ID's en de naam van de desbetreffende mbo-instelling. De kandidaat ID is afkomstig uit Remindo en is aangemaakt ten behoeve van het examenmoment. Beoordelaars ontvangen een link waarmee een account kan worden aangemaakt, ook hier is een koppeling met SSO. Er is ook een rol 'coördinator mbo-instelling'. Voor het aanmaken van een nieuw account vult een medewerker de volgende gegevens in: voornaam, achternaam, tussenvoegsel, e-mailadres, mbo-instelling en rol.

3.2 Persoonsgegevens

Deze paragraaf beschrijft alle persoonsgegevens die worden verwerkt, alsmede hoe deze persoonsgegevens worden gekwalificeerd en wat de bron is van deze gegevens. Hierbij is een onderscheid gemaakt tussen de persoonsgegevens die worden verwerkt door middel van Remindo en MijnRekenPortfolio/Skillsly enerzijds en de persoonsgegevens die worden verwerkt door middel van de Beoordelaarsmodule anderzijds.

Persoonsgegevens die worden verwerkt door leverancier Paragin door middel van Remindo en MijnRekenPortfolio/Skillsly

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatie-nummer)	Bron
Studenten	NAW-gegevens	Aanhef (geslacht)	Gewoon en eventuele bijzondere persoonsgegevens die worden verwerkt indien de student faciliteiten nodig heeft	Student informatie systeem ('SIS') Studenten Remindo MijnRekenPortfolio/Skillsly
	Contactgegevens	Voornaam		
	Studiegegevens	Tussenvoegsel		
	Examenresultaten	Achternaam		
	Online identicator	Emailadres		
	Gezondheidsgegevens	Codering (optioneel)		
		Gebruikerstaal		
		Geboortedatum		
		Adres (optioneel)		
		Postcode (optioneel)		
		Plaats (optioneel)		
		Land (optioneel)		

		Telefoonnummer (optioneel)		
		Mobiel telefoonnummer (optioneel)		
		Naam studierichting		
		Studentennummer		
		Organisatorische eenheid		
		Onderwijsinstelling		
		Klas		
		Examenresultaten		
		Aantal examens		
		Opleidingscode		
		Gebruikersnaam		
		Wachtwoord		
		IP-adres		
		Remindo kandidaat ID		
		Remindo testmoment ID		
		Gezondheidsgegevens (faciliteiten i.v.m. beperking)		
Medewerkers mbo-instellingen ⁷	NAW-gegevens	Aanhef (geslacht)	Gewoon	Medewerkers
	Contactgegevens	Voornaam		Remindo
	Personeelsnummer	Tussenvoegsel		MijnRekenPortfolio/Skillsl
	Online identicator	Achternaam		y
		Emailadres		
		Codering (optioneel)		
		Gebruikerstaal		
		Geboortedatum		

⁷ Onder 'medewerkers' worden alle personen geschaard die onder het gezag van de mbo-instelling persoonsgegevens verwerken in de breedste zin van het woord.

Adres (optioneel)

Plaats (optioneel)

Postcode
(optioneel)

Land (optioneel)

Telefoon
(optioneel)

Mobiel
telefoonnummer
(optioneel)

Organisatorische
eenheid

Onderwijsinstelling

Rol

Personeelsnummer

Remindo
beoordelaar ID

IP-adres

Gebruikersnaam

Wachtwoord

Medewerkers CEM ⁸	Contactgegevens	Naam	Gewoon	Medewerkers
	Online identicator	Emailadres		Remindo
		Organisatorische eenheid		MijnRekenPo rtfolio/Skillsl y
		IP-adres		
		Gebruikersnaam		
		Wachtwoord		

⁸ Medewerkers van de CEM in de functie van Hoofd Productie, Managementassistent en medewerker helpdesk hebben ook accounts in Remindo voor het verkrijgen van toegang tot het examenplatform.

Persoonsgegevens die worden verwerkt door leverancier Stipp in de Beoordelaarsmodule

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatie-nummer)	Bron
Studenten	Studiegegevens	Voornaam	Gewoon en eventuele bijzondere persoonsgegevens die worden verwerkt indien de student faciliteiten nodig heeft)	Remindo
	Examenresultaten	Tussenvoegsel		MijnRekenPortfolio/Skillsl y
	Online identicator	Achternaam		Beoordelaars module
	Gezondheidsgegevens	Onderwijsinstelling		
		Naam studierichting		
		Studentennummer		
		Examenresultaten		
		Aantal examens		
		Remindo kandidaat ID		
		Remindo testmoment ID		
		Gebruikersnaam		
		Wachtwoord		
		Gezondheidsgegevens (faciliteiten i.v.m. beperking)		
Medewerkers mbo-instellingen ⁹	Contactgegevens	Voornaam	Gewoon	Medewerkers
	Personeelsnummer	Tussenvoegsel		De Beoordelaars module
	Beschikbaarheid	Achternaam		
	Online identicator	Emailadres		
		Organisatorische eenheid		
		Mbo-instelling		

⁹ Onder 'medewerkers' worden alle personen geschaard die onder het gezag van de mbo-instelling persoonsgegevens verwerken in de breedste zin van het woord.

Rol
Beschikbaarheid
IP-adres
Gebruikersnaam
Wachtwoord

Bovenstaande biedt een overzicht van de persoonsgegevens die (mogelijk) verwerkt worden door de CEM in haar rol als verwerker ten opzichte van de mbo-instellingen. Dit betreft namelijk een indicatie gebaseerd op de mogelijkheden die de examenomgeving in Remindo en de Beoordelaarsmodule in Stipp bieden. Dit overzicht is opgesteld aan de hand van de ontvangen documentatie en de informatie die is verzameld gedurende de demonstratie en (inventarisatie)gesprekken. Welke persoonsgegevens precies verwerkt worden in de examenomgeving in Remindo, is afhankelijk wat de beheerders van de mbo-instellingen instellen in de eigen afnameomgeving. De gegevens die Cito ophaalt uit Remindo zijn geanonimiseerd.

De persoonsgegevens kunnen op meerdere manieren in Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule komen. Zo is het mogelijk om studentgegevens vanuit het SIS/LAS geautomatiseerd via koppelvlakken ('OO API') in Remindo en MijnRekenPortfolio/Skillsly te laten komen. Een andere optie is dat medewerkers zelf informatie toevoegen aan Remindo en MijnRekenPortfolio/Skillsly, rechtstreeks of via een Excel import.

Cito gebruikt voor de uitvoering van het onderzoek en analyses op de afgenomen (reken)examens voor de verbetering en normering van de (reken)examens anonieme examendata. Bij de (reken)examen prestaties staat een User ID en Session ID van de kandidaten, welke voor Cito beide niet herleidbaar zijn tot de kandidaten die de (reken)examens hebben afgelegd. Gegeven zijn pas persoonsgegevens als hiermee een natuurlijk persoon te identificeren is.¹⁰ Daar is in dit geval geen sprake van.

De precieze verwerking van persoonsgegevens is afhankelijk van de mbo-instelling. De mbo-instellingen hebben immers een bepaalde vrijheid met betrekking tot het gebruik van Remindo en MijnRekenPortfolio/Skillsly. De mbo-instelling blijft verantwoordelijk voor de verwerking en heeft uiteindelijk zeggenschap over welke persoonsgegevens er wel/niet verwerkt worden via Remindo en MijnRekenPortfolio/Skillsly.

3.3 Gegevensverwerkingen

Deze paragraaf geeft alle gegevensverwerkingen weer en de categorieën verwerkte persoonsgegevens per gegevensverwerking.

Gegevensverwerking	Categorieën persoonsgegevens
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens.	Gewone persoonsgegevens (zie onderdeel 2 'Persoonsgegevens').

¹⁰ Artikel 4 lid 1 AVG.

De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens. Gewone en mogelijk bijzondere persoonsgegevens (zie onderdeel 2 'Persoonsgegevens').

Om de rechtmatigheid van de gegevensverwerking te kunnen beoordelen, is het noodzakelijk om de gegevensverwerking in beeld te hebben die plaatsvinden binnen de reikwijdte van de CEM in haar rol als verwerker ten opzichte van de mbo-instellingen.

De gegevensverwerkingen die hier centraal staan zijn de verwerking van gewone persoonsgegevens van medewerkers ten behoeve van het plannen en vaststellen van de (reken)examens, en de verwerking van gewone en mogelijk bijzondere persoonsgegevens van studenten en medewerkers ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens

De persoonsgegevens kunnen op meerdere manieren in Remindo en MijnRekenPortfolio/Skillsly terechtkomen. Wanneer er een gekoppelde applicatie is die als bron kan dienen voor de persoonsgegevens, zoals een SIS of LAS, is het mogelijk om vanuit die systemen persoonsgegevens te sturen naar Remindo en MijnRekenPortfolio/Skillsly. Een andere optie is dat medewerkers zelf informatie toevoegen aan Remindo en MijnRekenPortfolio/Skillsly. Examengegevens komen in Remindo en MijnRekenPortfolio/Skillsly, doordat de studenten (reken)examens en metingen afnemen. De persoonsgegevens van medewerkers komen handmatig door medewerkers zelf in de Beoordelaarsmodule van Stipp. Daarnaast komen enkele persoonsgegevens van studenten bij leverancier Stipp terecht via Remindo en de logging tijdens de examenafname.

3.4 Technieken en methoden van de gegevensverwerkingen

Deze paragraaf beschrijft op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt.

Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule zijn cloud/SaaS-oplossingen. Onder een cloudoplossing wordt verstaan: het inzetten van een groot netwerk van servers die aan elkaar gekoppeld zijn om specifieke functies uit te voeren, zoals het opslaan en beheren van gegevens, het uitvoeren van toepassingen of het streamen van audiovisuele content. Het voordeel van een SaaS-oplossing is dat het schaalbaar is, het plaatsvindt op een virtuele infrastructuur en met relatief gemak uitgebreid kan worden.¹¹ Dit brengt echter ook risico's met zich mee. Het is daarom belangrijk dat CEM en Stipp contractuele afspraken maken met leverancier Paragin over de verwerking van persoonsgegevens. Onder het kopje 'Risico's voor betrokkenen' en 'Maatregelen' wordt hier verder op ingegaan.

¹¹ Uitleg bij het Rijksmodel, p. 46.

3.5 Verwerkingsdoeleinden

Deze paragraaf beschrijft de doeleinden van de verwerkingen.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens.	Het klaarzetten van digitale (reken)examens, zodat de kandidaat het (reken)examen kan maken. Het vaststellen van de (reken)examens vooraf aan de afname door de examencommissie (wettelijk verplicht voor de mbo-instelling).	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan Remindo en MijnRekenPortfolio/Skillsly gekoppelde systemen: het kunnen bieden van onderwijs, het uitvoering geven aan de inschrijving en het in staat stellen van studenten tot het behalen van een diploma.
De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	Het toewijzen van geplande (reken)examens aan kandidaten voor afname. Beoordeling van afnames door examinatoren. Registreren van resultaten en inzage door kandidaten in gemaakt werk. Communiceren resultaat. Psychometrische en inhoudelijke analyse van gegevens (reken)examen met kwaliteitsverbetering als doel.	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule van Stipp gekoppelde systemen: het kunnen bieden van onderwijs, het uitvoering geven aan de inschrijving en het in staat stellen van studenten tot het behalen van een diploma.

De mbo-instelling is de verwerkingsverantwoordelijke in de zin van de AVG, zoals vastgesteld in onderdeel 6 'Betrokken partijen'. Als verwerkingsverantwoordelijke heeft de mbo-instelling de zeggenschap over de verwerking van persoonsgegevens, en heeft deze het doel en de middelen van de gegevensverwerking vastgesteld.

De CEM is de verwerker in de zin van de AVG, zoals vastgesteld in onderdeel 6 'Betrokken partijen' en heeft daarom geen zeggenschap over het doel en de middelen van de gegevensverwerking. De mbo-instelling bepaalt het doel en de middelen van de gegevensverwerking, en het is aan de CEM om slechts in opdracht van de mbo-instelling persoonsgegevens te verwerken. Paragin en Stipp zijn, als leveranciers van de SaaS-oplossingen Remindo en MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule, aan te merken als subverwerker in de zin van de AVG, zoals vastgesteld in paragraaf 6 'Betrokken partijen' en heeft geen zeggenschap over het doel en de middelen van de gegevensverwerking.

Persoonsgegevens mogen enkel worden gebruikt voor het doel waarvoor ze zijn verzameld, of voor doeleinden die daarmee verenigbaar zijn.¹² Dit betekent bijvoorbeeld dat persoonsgegevens van studenten in principe alleen mogen worden gebruikt om de overeenkomst uit te voeren (om het onderwijs aan te bieden), tenzij het doel verenigbaar is. Het plannen, vaststellen, afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens is hier onderdeel van. Het is niet toegestaan om deze gegevens voor andere, onverenigbare doeleinden, te gebruiken.

Voor het proces rondom de uitvoering van de (reken)examens is het van belang om een duidelijk onderscheid te maken tussen het doel om de gegevens te verwerken en de middelen om de gegevens te verwerken. Het doel van de verwerking is waarom de persoonsgegevens worden verwerkt. Het doel van de verwerking is kortgezegd de het faciliteren van (reken)examens door het plannen, vaststellen, afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens. De middelen van de verwerking zien op de manier waarop de verwerking praktisch vorm krijgt, in dit geval het gebruik van Remindo, MijnRekenPortfolio/Skillsly, de Beoordelaarsmodule en het uitvoeren psychometrische analyses op de examendata.

3.6 Betrokken partijen

Deze paragraaf beschrijft alle partijen welke mogelijk betrokken zijn, alsmede welke rol deze vervullen, onderverdeeld in: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend is tevens benoemd welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens.

De CEM heeft in haar rol als verwerker ten opzichte van de mbo-instellingen, diverse partijen ingeschakeld als subverwerker. Ten behoeve van het vaststellen van de verantwoordelijkheden van de betrokken partijen bij de verwerking van persoonsgegevens, dient allereerst te worden vastgesteld wie in deze verhouding de verwerkingsverantwoordelijke is. Het vaststellen van de privacyrechtelijke rolverdeling is met name van belang aangezien de verwerkingsverantwoordelijke verplicht is om de verwerking van persoonsgegevens te baseren op een hiervoor geschikte verwerkingsgrondslag uit de AVG. Ook zal de verwerkingsverantwoordelijke zorg moeten dragen voor de juiste toepassing van de verwerkingsbeginselen, zoals opgenomen in artikel 5 AVG.

De partij die het doel en de middelen van de verwerking vaststelt wordt gezien als de verwerkingsverantwoordelijke in de zin van de AVG. Partijen die gegevens in opdracht van de verwerkingsverantwoordelijke verwerken zijn de verwerkers. Partijen die gegevens verwerken ten behoeve van de verwerker worden aangemerkt als subverwerkers.

De mbo-instelling is ten aanzien van de gegevensverwerking door de CEM aan te merken als verwerkingsverantwoordelijke. De mbo-instelling bepaalt immers het doel en de middelen van de gegevensverwerking door de CEM. De CEM wordt ingeschakeld door de mbo-instelling om de gegevensverwerking te verrichten. De CEM verwerkt dus in opdracht van de mbo-instelling de persoonsgegevens en is dus aan te merken als verwerker in de zin van de AVG.

¹² Artikel 5 (1) (b) Algemene verordening gegevensbescherming.

Zoals blijkt uit de verwerkersovereenkomst die wordt gehanteerd, schakelt de CEM op haar beurt twee subverwerkers in: Paragin en Stipp.

Paragin wordt ingezet voor de levering van Remindo en MijnRekenPortfolio/Skillsly en OnTrac¹³. Hoewel de mbo-instellingen een eigen afnameomgeving in Remindo en MijnRekenPortfolio/Skillsly hebben, kan de servicedesk van Paragin wel in deze schooleigen omgeving voor hulpvragen. Paragin verwerkt dus, in opdracht van de CEM, persoonsgegevens en kan daarom worden gekwalificeerd als subverwerker.

Daarnaast schakelt de CEM Stipp en Cito in. Cito kwalificeert zich als derde, omdat zij alleen anonieme examendata verwerken ten behoeve van psychometrische analyses voor kwaliteitsdoeleinden. Hier zijn geen persoonsgegevens bij betrokken. Stipp kwalificeert zich als subverwerker, doordat zij de Beoordelaarsmodule leveren waarin persoonsgegevens van medewerkers worden verwerkt. Daarnaast ontvangt Stipp een logging van de afgenomen (reken)examens in Remindo, waarin ook persoonsgegevens van studenten staan.

Paragin heeft Amazon Web Services ('AWS') ingeschakeld ten behoeve van hosting van Remindo en MijnRekenPortfolio/Skillsly. AWS verwerkt dus in opdracht van Paragin persoonsgegevens. Daarnaast schakelt Paragin Cloutive Technology Services B.V. ('Cloutive') in voor de infrastructuur. Cloutive heeft toegang tot de persoonsgegevens en kan proactief handelen bij bijvoorbeeld pieken in het dataverkeer of DDoS aanvallen. Cloutive is daarom een subsubverwerker van Paragin.

Tot slot dienen de studenten en medewerkers van de mbo-instellingen en de CEM te worden aangemerkt als betrokkenen.

Schematisch leidt dit tot het onderstaande overzicht, waarin de hierboven beschreven rolverdeling en werkzaamheden schematisch zijn weergegeven.

Naam partij	Rol partij	Functionies/afdelingen	Persoonsgegevens
Mbo-instelling	Verwerkingsverantwoordelijke	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
CEM	Verwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
Paragin	Subverwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
Stipp	Subverwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
Cito	Derde	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
AWS	Subsubverwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens

¹³ OnTrac valt buiten de scope van deze DPIA. Ten aanzien van OnTrac is eerder een DPIA uitgevoerd door ICTRecht in opdracht van de MBO Raad.

Cloutive	Subsubverwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
SIS/LAS	Verwerker	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
Federatief inloggen (waaronder SURFconext en Kennisnet Entree)	Verwerker	n.v.t.	Gewone persoonsgegevens
Studenten	Betrokkenen	n.v.t.	Gewone en mogelijk bijzondere persoonsgegevens
Medewerkers van mbo-instellingen	Betrokkenen	n.v.t.	Gewone persoonsgegevens

3.7 Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

Betrokken Partij	Belangen
Mbo-instelling	- Voorzien in onderwijs - Bedrijfsbelangen - Financiële en commerciële belangen
CEM	- Voorzien in (reken)examens - Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan overeenkomst met de mbo-instelling
Paragin	- Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan overeenkomst met de CEM
Stipp	- Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan overeenkomst met de CEM
Cito	- Organisatiebelang - Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan overeenkomst met de CEM
AWS	- Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan overeenkomst met Paragin

Cloutive	• Bedrijfsbelangen • Financiële en commerciële belangen • Voldoen aan overeenkomst met Paragin
Studenten	• Volgen van onderwijs aan mbo-instelling(en)
Medewerkers mbo-instellingen en CEM	• Uitvoeren van werkzaamheden voor mbo-instelling(en) en CEM in het kader van de arbeidsovereenkomst

3.8 Verwerkingslocaties

Deze paragraaf benoemt in welke landen de gegevensverwerkingen plaatsvinden, alsmede eventuele doorgiftemechanismen indien verwerkingen buiten de EER plaatsvinden en welke maatregelen daarvoor van toepassing zijn.

Gegevensverwerkingen	Verwerkingslocaties	Doorgiftemechanismen	Maatregelen
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens. De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	Opslag en verwerking persoonsgegevens: • Nederland – Paragin, Cloutive en Stipp • Duitsland (Frankfurt) – Amazon Web Services	n.v.t.	n.v.t.

Wanneer persoonsgegevens worden doorgegeven aan een land buiten de Europese Economische Ruimte ('EER'), dient gewaarborgd te zijn dat ook deze verwerking aan de vereisten van de AVG voldoet en de persoonsgegevens dezelfde bescherming genieten als binnen de EER. Persoonsgegevens mogen daarom enkel verwerkt of doorgegeven worden aan landen buiten de EER met een adequaat beschermingsniveau of wanneer er passende waarborgen aanwezig zijn.

Paragin is een in Nederland gevestigde organisatie. Zij maakt gebruik van twee subverwerkers. Amazon Web Services ('AWS') en Cloutive Technology Services B.V. ('Cloutive'). AWS is gevestigd buiten de EER maar op 10 juli 2023 is het 'EU-US Data Privacy Framework' aangenomen door de Europese Commissie. De VS wordt nu gezien als een land met een adequaat beschermingsniveau, waardoor het sluiten van *Standard Contractual Clauses* (SCC's) niet meer nodig is. Het is wel vereist dat AWS

is aangesloten bij het Data Privacy Framework. Op het moment van schrijven is AWS aangesloten. De hosting vindt fysiek plaats binnen de EER, namelijk in Frankfurt in Duitsland. Cloutive wordt door Paragin ingeschakeld ten behoeve van de IT-infrastructuur. Cloutive is gevestigd in Amsterdam en is dus een in Nederland gevestigde organisatie.

Daarnaast is Stipp als verwerker gevestigd in Deventer en ook een in Nederland gevestigde organisatie.

3.9 Juridisch en beleidsmatig kader

Deze paragraaf beschrijft alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn¹⁴ zijn niet genoemd.

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens.	Wet educatie en beroepsonderwijs, Model documentair structuurplan	De rekentoets is geregeld in diverse onderwijssectorwetten. In het kader van het mbo is dit vastgelegd in art. 7.4.11 derde lid van de WEB of voor een centraal examen voor het onderdeel rekenen in het mbo krachtens art. art. 4.7.3 jo. 7.4.3a, tweede lid, WEB.
De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.		

Wet educatie en beroepsonderwijs

De Wet educatie en beroepsonderwijs ('WEB') regelt verschillende vormen van beroepsonderwijs en volwasseneneducatie, waaronder het middelbaar beroepsonderwijs ('mbo'). Van belang voor verwerkingen door de CEM in haar rol als verwerker is dat de WEB bepalingen bevat omtrent de examinering, het informeren van studenten daarover en de inschrijving van studenten voor examenvoorzieningen.

Ten aanzien van de verwerkingen die plaatsvinden in het kader van het examineringsproces, zijn de mbo-instellingen die de CEM inschakelen zelf verwerkingsverantwoordelijke.

¹⁴ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

3.10 Bewaartermijnen

Deze paragraaf beschrijft de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden en zet de mogelijke vernietiging of archivering aan het einde van de bewaartermijn uiteen.

Gegevensverwerking	Verwerking doeleinde	Categorie Persoonsgegevens	Bewaartermijn	Motivatie bewaartermijn
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens.	Het klaarzetten van digitale (reken)examens, zodat de kandidaat het (reken)examen kan maken. Het vaststellen van de (reken)examens vooraf aan de afname door de examencommissie (wettelijk verplicht voor de mbo-instelling).	Zie paragraaf 2.2.	[in te vullen door de mbo-instelling] De maximale bewaartermijn betreft 10 jaar of korter indien gewenst door de mbo-instelling.	[in te vullen door de mbo-instelling] De maximale bewaartermijn betreft 10 jaar of korter indien gewenst door de mbo-instelling.
De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	Het toewijzen van geplande (reken)examens aan kandidaten voor afname. Beoordeling van afnames door examinatoren. Registreren van resultaten en inzage door kandidaten in gemaakt werk. Communiceren en resultaat.			

	Psychometrische en inhoudelijke analyse van gegevens (reken)examen met kwaliteitsverbetering als doel.			
--	--	--	--	--

Invoer en handhaving bewaartermijnen

Remindo bevat verschillende opties met betrekking tot het opschonen van oude resultaten. Resultaten kunnen automatisch worden geanonimiseerd na 1 t/m 10 jaar, of nooit. De resultaten worden dus maximaal 10 jaar bewaard.

De lijst met logging gegevens die Stipp ontvangt per afgenomen (reken)examen, wordt volgens Stipp per jaar ongeschoond. Er zijn hier geen specifieke afspraken over gemaakt met de CEM.

Toelichting bewaartermijnen

Zoals gezegd worden de persoonsgegevens die te vinden zijn in Remindo en MijnRekenPortfolio/Skillsly veelal uit andere systemen ingeladen. Dit betekent dat dezelfde persoonsgegevens op meer dan één locatie worden bewaard, en er dus ook verschillende bewaartermijnen kunnen gelden voor persoonsgegevens die zijn opgeslagen in deze in Remindo en MijnRekenPortfolio/Skillsly en persoonsgegevens die worden opgeslagen in bronsystemen zoals het SIS.

De maximale bewaartermijn betreft 10 jaar na diplomering. Indien gewenst kan de mbo-instelling een kortere bewaartermijn instellen, tussen de 1 en 10 jaar na diplomering. Wij adviseren de mbo-instellingen om de resultaten niet langer te bewaren dan noodzakelijk.

4. Beoordeling rechtmatigheid gegevensverwerkingen

In dit hoofdstuk wordt de rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen en rechten van de betrokkene beoordeeld.

4.1 Rechtsgrond

De AVG vereist dat de verwerkingsverantwoordelijke een rechtmatige grondslag heeft voor het verwerken van persoonsgegevens.

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens. De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	Uitvoering van de overeenkomst	De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens is noodzakelijk voor de uitvoering van de inschrijving voor het onderwijs bij de desbetreffende mbo-instelling. Het bieden van de mogelijkheid tot het behalen van het (reken)examen vormt onderdeel van die inschrijving. De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens is eveneens noodzakelijk voor de uitvoering van de inschrijving voor het onderwijs en voor de uitvoering van de arbeidsovereenkomst met de betrokken medewerker.

Toelichting grondslag

De enige grondslag die de beoogde verwerking kan dragen, is de uitvoering van de overeenkomst. Ten aanzien van studenten zijn de verwerkingen noodzakelijk om uitvoering te geven aan de inschrijving bij de desbetreffende mbo-instelling. De verwerking van persoonsgegevens van medewerkers is noodzakelijk voor de uitvoering van de arbeidsovereenkomst met de desbetreffende medewerker.

4.2 Bijzondere persoonsgegevens

Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. In deze paragraaf wordt beoordeeld of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is.

Binnen Remindo en MijnRekenPortfolio/Skillsly kan bij studenten onder het 'toegankelijkheidsprofiel' veld een keuze worden gemaakt tussen verschillende opties. Hierbij kan worden gekozen voor extra tijd op basis van verschillende redenen zoals voor blinden, slechtzienden of gewoon extra tijd zonder aanvullende reden (zoals dyslexie of dyscalculie). Deze gegevens over extra tijd staan vervolgens ook in de logging per afgenomen (reken)examen van Stipp. Dit betreffen gezondheidsgegevens, zodat een uitzonderingsgrond voor de verwerking van deze gegevens aanwezig dient te zijn.

Deze uitzonderingsgrond kan gevonden worden in art. 9 lid 2 sub g AVG jo. art. 30 lid 2 sub a AVG. De verwerking is namelijk noodzakelijk met het oog op de speciale begeleiding van studenten of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand.

Gegevensverwerking	Type bijzonder persoonsgegeven	Uitzonderingsgrond
De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	Gezondheidsgegevens	Art. 9 lid 2 sub g AVG jo. art. 30 lid 2 sub a AVG.

4.3 Doelbinding

In deze paragraaf wordt de toelaatbaarheid van eventuele (nieuwe) verdere verwerkingen op grond van Unie- of lidstaatrechtelijk, dan wel het oorspronkelijke verwerkingsdoeleinde beschreven.

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
De verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens.	NAW-gegevens Contactgegevens Personeelsnummer Online identicator	Het klaarzetten van digitale (reken)examens, zodat de kandidaat het (reken)examen kan maken. Het vaststellen van	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan Remindo en

		de (reken)examens vooraf aan de afname door de examencommissie (wettelijk verplicht voor de mbo-instelling).	MijnRekenPortfolio/Skillsly gekoppelde systemen: het kunnen bieden van onderwijs, het uitvoering geven aan de inschrijving en het in staat stellen van studenten tot het behalen van een diploma.
De verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens.	NAW-gegevens Contactgegevens Online identicator Personeelsnummer Studiegegevens (studentennummer) Examenresultaten Gezondheidsgegevens	Het toewijzen van geplande (reken)examens aan kandidaten voor afname. Beoordeling van afnames door examinatoren. Registreren van resultaten en inzage door kandidaten in gemaakt werk. Communiceren resultaat. Psychometrische en inhoudelijke analyse van gegevens (reken)examen met kwaliteitsverbering als doel.	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule van Stipp gekoppelde systemen: het kunnen bieden van onderwijs, het uitvoering geven aan de inschrijving en het in staat stellen van studenten tot het behalen van een diploma.

In Remindo en MijnRekenPortfolio/Skillsly (Paragin) kunnen reeds voorhanden persoonsgegevens van studenten uit gekoppelde applicaties (SIS of LAS) of via een Excel import worden ingeladen. Daarnaast is het mogelijk om studenten en medewerkers van de mbo-instelling met hun eigen instellingsaccount te laten inloggen via SSO, zodat de bestaande accountsgegevens (her)gebruikt worden. Dat geldt ook voor medewerkers die inloggen in de Beoordelaarsmodule (Stipp). Verder ontvangt Stipp door middel van logging per afgenomen (reken)examen gegevens van de studenten, zoals voornaam, achternaam, naam van de mbo-instelling, extra tijd en type (gezondheidsgegevens), studiegegevens en alle gegevens omtrent het afgenomen (reken)examen. Voor de beoordelaars is in de Beoordelaarsmodule alleen

de kandidaat ID, testmoment ID en naam van de mbo-instelling van de student zichtbaar.

Omdat de persoonsgegevens al verwerkt werden door mbo-instellingen, doet zich de vraag voor of de verwerking van persoonsgegevens ten behoeve van het plannen, vaststellen, afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens rondom het examineringsproces verenigbaar is met het doel of de doeleinden waarvoor de al voorhanden gegevens oorspronkelijk werden verwerkt. Indien dat het geval is, hoeft voor deze verwerkingen geen nieuwe grondslag te gezocht, maar vindt de verwerking plaats binnen de grondslag van de verwerking voor het oorspronkelijke doel.

Om te beoordelen of een verwerkingsdoel verenigbaar is met het oorspronkelijke verwerkingsdoel, moet op de volgende punten worden gelet:

- het verband tussen het oorspronkelijke doel en het nieuwe/toekomstige doel;
- de context waarin de gegevens zijn verzameld (wat is de relatie tussen uw onderneming/organisatie en de persoon?);
- de soort en aard van de gegevens (betreft het gevoelige gegevens?);
- de mogelijke gevolgen van de voorgenomen verdere verwerking (welke zijn de gevolgen de betrokkene?);
- het bestaan van passende waarborgen (zoals versleuteling of pseudonimisering).

Aangezien het oorspronkelijke doeleinde van de **verwerking van al beschikbare gegevens** plaatsvond op grond van de inschrijving (uitvoering van de overeenkomst) met als overkoepelende doelen het kunnen bieden van onderwijs, het uitvoering geven aan de inschrijving en het in staat stellen van studenten tot het behalen van een diploma, zal de beoogde verwerking verenigbaar zijn.

Het nieuwe doeleinde (plannen, vaststellen, afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens) is onlosmakelijk deel van het kunnen realiseren van de oorspronkelijke doeleinden. Aangezien hoofdzakelijk 'gewone' persoonsgegevens worden verwerkt, en bijzondere persoonsgegevens enkel incidenteel worden verwerkt als een betrokkene deze verstrekt (aan de mbo-instelling voor extra tijd tijdens het (reken)examen), leidt de aard van de gegevens niet tot een andere conclusie. Tot slot zijn de gevolgen voor betrokkenen gering, en hebben Paragin en Stipp passende beveiligingsmaatregelen getroffen voor Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule. Zo krijgt de CEM of Paragin alleen in geval van nood of na toestemming toegang tot de eigen digitale afnameomgeving in Remindo en MijnRekenPortfolio/Skillsly. Daarnaast vindt de beoordeling van een (reken)examen door een beoordelaar van een andere mbo-instelling anoniem plaats, waardoor de identificeerbaarheid van de studenten beperkt is. De verdere verwerking van deze persoonsgegevens is dus verenigbaar.

Ten aanzien van medewerkers van de mbo-instelling valt de verenigbaarheidstoets eveneens positief uit ten aanzien van **al verwerkte persoonsgegevens**. De persoonsgegevens van medewerkers werden oorspronkelijk verwerkt om uitvoering te kunnen geven aan de arbeidsovereenkomst en de medewerkers in staat te stellen hun werkzaamheden uit te voeren. De nieuwe verwerking maakt daar onlosmakelijk deel van uit. Ook in dit geval leiden de aard van de persoonsgegevens, de mogelijke gevolgen van de verwerking en het bestaan van passende waarborgen niet tot een andere conclusie, zodat dus wederom sprake is van een verenigbare verwerking.

Voor wat betreft persoonsgegevens **die niet eerder werden verwerkt**, zoals de examenresultaten, online identificators en gezondheidsgegevens van de studenten speelt verenigbaarheid van de verwerking geen rol. Dat geldt ook voor de NAW-gegevens, contactgegevens, beschikbaarheid en online identificators van de medewerkers die zij zelf invoeren in Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule. Voor deze verwerkingen wordt teruggevallen op de grondslag 'uitvoering van de overeenkomst', zoals toegelicht onder paragraaf 3.1.

4.4 Noodzaak en evenredigheid

De AVG eist dat persoonsgegevens enkel verwerkt worden voor zover dat noodzakelijk is om het beoogde doel te bereiken. Dit wordt ook wel het beginsel van dataminimalisatie genoemd. Bij het toetsen van de noodzakelijkheid van persoonsgegevens wordt gekeken naar proportionaliteit en subsidiariteit. Het verwerken van persoonsgegevens dient noodzakelijk te zijn om het geïdentificeerde doel te bereiken. Daarbij moeten er zo min mogelijk persoonsgegevens verwerkt te worden. Daarnaast moet het doel niet op een minder ingrijpende manier bereikt kunnen worden.

In deze DPIA worden twee overkoepelende gegevensverwerking onderscheiden. Allereerst de verwerking van medewerkersgegevens ten behoeve van het plannen en vaststellen van de (reken)examens met als verwerkingsdoeleinde het klaarzetten van digitale (reken)examens, zodat de kandidaat het (reken)examen kan maken en het vaststellen van de (reken)examens vooraf aan de afname door de examencommissie (wettelijk verplicht voor de mbo-instelling). De tweede gegevensverwerking ziet op de verwerking van persoonsgegevens van de student en medewerker van de mbo-instelling en de CEM ten behoeve van het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens. Deze gegevensverwerking heeft als verwerkingsdoeleinde het toewijzen van geplande (reken)examens aan kandidaten voor afname, beoordeling van afnames door examinatoren, registreren van resultaten en inzage door kandidaten in gemaakt werk, communiceren van resultaat en psychometrische en inhoudelijke analyse van gegevens van (reken)examens met kwaliteitsverbetering als doel.

In deze paragraaf zal ten aanzien van deze verwerkingsdoeleinden worden beoordeeld of de verwerking noodzakelijk en evenredig is voor het verwezenlijken van deze doeleinden. Indien de mbo-instelling aanvullende verwerkingsdoeleinden bepaalt, dient zij steeds te beoordelen of er sprake is van noodzakelijkheid en evenredigheid.

Gegevensverwerking 1

Proportionaliteit

Ten aanzien van de verwerking van persoonsgegevens van de medewerker van de mbo-instelling ten behoeve van het plannen en vaststellen van de (reken)examens kan de vraag worden gesteld of de verwerking van adresgegevens noodzakelijk zijn. Voor het inplannen en vaststellen van digitale (reken)examens zijn adresgegevens (adres, plaats, postcode, land) van medewerkers niet noodzakelijk. Dat betekent dat voor dit onderdeel van de verwerking nog niet wordt voldaan aan het proportionaliteitsbeginsel.

Subsidiariteit

Zoals hierboven opgemerkt is de verwerking van adresgegevens van medewerkers niet proportioneel. Bovendien kan het doel van de verwerking ook op een minder ingrijpende manier worden bereikt, zonder de verwerking van adresgegevens.

De verwerking van persoonsgegevens is derhalve voor een deel niet noodzakelijk.

Gegevensverwerking 2

Proportionaliteit

Ten aanzien van proportionaliteit bij de tweede gegevensverwerking, dient allereerst te worden opgemerkt dat de studentgegevens die in Remindo en MijnRekenPortfolio/Skillsly verwerkt worden, grotendeels al bekend zijn bij de onderwijsinstellingen. Deze gegevens worden geïmporteerd uit andere systemen zoals het SIS. De gegevens uit het SIS worden in Remindo en MijnRekenPortfolio/Skillsly verrijkt met gegevens van studenten over examenresultaten en online identificatoren. De meeste gegevens van medewerkers worden door de medewerkers zelf in Remindo, MijnRekenPortfolio/Skillsly en de Beoordelaarsmodule geregistreerd. Mbo-instellingen kunnen zelf instellen welke optionele gegevens van studenten en medewerkers worden geregistreerd in Remindo en MijnRekenPortfolio/Skillsly.

Niet alle gegevens die worden verwerkt van studenten en medewerkers bij afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens zijn noodzakelijk. Zo is de verwerking van NAW-gegevens van medewerkers en studenten van de mbo-instelling en de CEM in Remindo en MijnRekenPortfolio/Skillsly deels niet noodzakelijk. Het gaat daarbij specifiek om de verwerking van adresgegevens, zoals het adres, plaats, postcode, land. De verwerking hiervan is optioneel, zodat mbo-instellingen zelf de doeleinden van de verwerking ervan moeten bepalen en vastleggen. Daarnaast is de logging door Stipp van de afgenomen (reken)examens inzichtelijk voor medewerkers van de CEM en Stipp. Voor wat betreft de verwerking van de gezondheidsgegevens van studenten (extra tijd, type blind/slechtziend) die hierin staan, kan worden gesteld dat de verwerking hiervan door Stipp niet noodzakelijk is om het doel te bereiken.

Subsidiariteit

Ook zonder de verwerking van de adresgegevens van medewerkers en studenten in Remindo en MijnRekenPortfolio/Skillsly kan het doel van de gegevensverwerking worden bereikt. Dat geldt ook voor de verwerking van contactgegevens. Er is dus een minder ingrijpende wijze om het doel te bereiken, waardoor deze verwerking niet aan subsidiariteit voldoet. De logging van Stipp voldoet ook niet aan subsidiariteit, nu het doel, het beoordelen van de (reken)examens ook kan worden bereikt zonder de gezondheidsgegevens met betrekking tot extra tijd.

Voor wat betreft de overige verwerkingen van persoonsgegevens van studenten en medewerkers van mbo-instellingen en de CEM kan het afnemen, beoordelen, analyseren, registreren, verlenen van inzage, communiceren en verbeteren van de (reken)examens niet plaatsvinden zonder deze persoonsgegevens. Er is dus geen minder ingrijpende wijze om het doel te bereiken, los van de staking van de verwerking van enkele van deze persoonsgegevens.

4.5 Rechten van betrokkenen

Deze paragraaf beschrijft de procedure waarmee invulling wordt gegeven aan de rechten van betrokkenen, en indien van toepassing op welke grondslag de rechten van betrokkenen worden beperkt.

Rechten van betrokkene	van	Procedure uitvoering	ter	Beperking op grond van wettelijke uitzondering
Recht van inzage		[mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]		n.v.t.
Recht rectificatie aanvulling	op en	[mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]		n.v.t.
Recht vergetelheid	op	Indien een betrokkene gebruik wenst te maken van het recht op vergetelheid, dan kan een verzoek worden ingediend bij Stipp, Paragin en/of de mbo-instelling, zodat de persoonsgegevens kunnen worden gewist. De mbo-instelling hoeft hier niet aan te voldoen indien de gegevens worden bewaard conform een wettelijke verplichting. [mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]		n.v.t.
Recht op beperking van de verwerking		Indien een betrokkene gebruik wenst te maken van het recht op dataportabiliteit, dan kan een verzoek worden ingediend bij Stipp, Paragin en/of de mbo-instelling, zodat de verwerking beperkt kan worden indien aan één van de in art. 18 AVG genoemde elementen is voldaan. [mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]		n.v.t.

Recht op dataportabiliteit	Indien een betrokkene gebruik wenst te maken van het recht op dataportabiliteit, dan kan een verzoek worden ingediend bij Stipp, Paragin en/of de mbo-instelling, zodat de persoonsgegevens gedeeld kunnen worden, indien aan de in art. 20 AVG genoemde elementen is voldaan. [mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]	n.v.t.
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	[mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]	n.v.t.
Recht om bezwaar te maken	Dit recht kan alleen worden ingeroepen indien de verwerking is gebaseerd op art. 6 lid 1 sub e jo. art. 6 lid 1 sub f AVG. Daar is in dit geval geen sprake van.	n.v.t.
Recht op duidelijke informatie	[mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]	n.v.t.

Op grond van de AVG hebben betrokkenen een aantal rechten ten aanzien van hun persoonsgegevens. Een verzoek van een betrokkene tot uitvoering van deze rechten is vormvrij en kan door een betrokkene bij zowel een verwerker (CEM) als een verwerkingsverantwoordelijke (mbo-instelling) worden ingediend. De verwerkingsverantwoordelijke (mbo-instelling) dient haar systemen zo te hebben ingericht dat binnen één maand aan een dergelijk verzoek kan worden voldaan. Is het verzoek complex, dan dient de verwerkingsverantwoordelijke binnen één maand mee te delen dat ze er binnen maximaal twee maanden op terugkomt. Voor het voldoen aan verzoeken van betrokkenen in het kader van hun wettelijke rechten, mogen in principe geen kosten worden gerekend.

Een betrokkene (medewerker of student) kan een verzoek indienen bij zowel de verwerkingsverantwoordelijke (mbo-instelling) als een verwerker (CEM) als een subverwerker (Paragin). Mocht een verzoek bij de CEM worden ingediend, dan is het aan de CEM om het verzoek door te sturen naar de desbetreffende mbo-instelling. Mocht een verzoek bij Paragin worden ingediend, dan is het aan Paragin om het verzoek door te sturen naar de CEM. De CEM dient dit verzoek vervolgens door te sturen aan de desbetreffende mbo-instelling. In de verwerkersovereenkomst worden passende afspraken gemaakt over het afhandelen van deze verzoeken.

Voor de afhandeling van rechten van betrokkenen dient de mbo-instelling een procedure vast te stellen en te hanteren.

5. Beschrijving en beoordeling risico's voor betrokkenen

In dit hoofdstuk worden de risico's van de gegevensverwerkingen beschreven en beoordeeld.

In onderstaande tabel zijn verschillende risico's beschreven in het kader van de verwerking van persoonsgegevens door de CEM. Bij elk risico is de kans dat er iets fout kan gaan met persoonsgegevens omschreven. Daarnaast is de impact omschreven, wat tezamen resulteert in een risico-inschatting. Hierbij is ingegaan op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Voor de inschatting van de kans, impact en het risico zijn de niveaus 'laag', 'gemiddeld' en 'hoog' gebruikt. Het risico wordt bepaald aan de hand van de formule kans x impact.

		Kans		
		laag	midden	hoog
Impact	hoog	laag	hoog	hoog
	midden	laag	midden	hoog
	laag	laag	laag	laag

Beschrijving risico	Kans	Impact	Risico-inschatting
Het risico bestaat dat het overzicht van verwerkte persoonsgegevens (het verwerkingsregister) binnen de mbo-instelling niet up-to-date is. Dit kan leiden tot situaties waarin	Laag	Midden	Laag

betrokkenen hun rechten niet kunnen uitoefenen, en tot het niet voldoen aan de verantwoordingsplicht die op mbo-instellingen als verwerkingsverantwoordelijke rust.			
---	--	--	--

De CEM beschikt op dit moment niet over een verwerkingsregister waarin de verwerkingen, die worden uitgevoerd in de hoedanigheid van verwerker, zijn opgenomen. Dit kan leiden tot een gebrek aan inzicht in verwerkingen die worden uitgevoerd ten behoeve van de mbo-instellingen en verhoogde risico's op onrechtmatige of onveilige gegevensverwerking.

Hoog Midden **Hoog**

Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen door CEM niet vooraf door mbo-instellingen zelf zijn vastgelegd, eveneens in het verwerkingsregister. Dat zou leiden tot een onrechtmatige verwerking die ook de uitoefening door betrokkenen van hun rechten kan belemmeren.

Laag Midden **Laag**

Binnen beide gegevensverwerkingen (het plannen/vaststellen en het afnemen/analyseren van (reken)examens) worden persoonsgegevens verwerkt die niet strikt noodzakelijk zijn voor het bereiken van het verwerkingsdoel. Het betreft hier onder meer de adresgegevens (adres, plaats, postcode, land) van medewerkers en studenten, alsook gezondheidsgegevens van studenten (zoals informatie over extra tijd of visuele beperkingen) die zichtbaar zijn in loggingfunctionaliteiten van Stipp. Verwerking van niet-noodzakelijke persoonsgegevens leidt tot een schending van het beginsel van dataminimalisatie zoals voorgeschreven door de AVG. Dit verhoogt het risico op

Midden Midden **Midden**

datalekken en ongeoorloofde toegang tot gevoelige informatie, met mogelijke reputatieschade en juridische gevolgen voor de mbo-instelling.

Het risico bestaat dat persoonsgegevens langer worden bewaard dan noodzakelijk. Dat risico kan ontstaan doordat ofwel geen bewaartermijn is vastgesteld ofwel doordat bewaartermijnen niet consequent worden gehandhaafd. Dat leidt tot een onrechtmatige verwerking van persoonsgegevens en tot een groter risico bij beveiligingsincidenten.	Laag	Midden	Laag
--	------	--------	------

Het risico bestaat dat er geen passende afspraken zijn gemaakt met partijen door wie persoonsgegevens worden verwerkt. Als dit niet, niet tijdig, of niet correct wordt gedaan, ontstaat het risico dat de ontvangende partij de persoonsgegevens onbehoorlijk verwerkt. Dit leidt voor betrokkenen tot het risico op misbruik van persoonsgegevens, datalekken, verlies van vertrouwelijkheid, en dat betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen.

Laag Hoog Laag

Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op de mbo-instellingen rust. Hierdoor kunnen betrokkenen niet verwachten en/of anticiperen op welke wijze de desbetreffende partijen met hun persoonsgegevens omgaan. Dit leidt ertoe dat betrokkenen hun rechten niet of minder goed kunnen uitoefenen.	Hoog	Laag	Laag
--	------	------	------

	Laag	Hoog	Laag
Het risico bestaat dat persoonsgegevens bij CEM ongeautoriseerd toegankelijk zijn, doordat geen encryptie wordt toegepast op data-at-rest en data-in-transit. Hoewel op onderdelen gegevens worden geanonimiseerd, zijn andere gegevens onvoldoende beschermd bij een beveiligingsincident. Dit kan ertoe leiden dat persoonsgegevens van betrokkenen bij verlies of diefstal van gegevens ongewenst worden ingezien, wat schade kan veroorzaken aan hun privacy.			

Het risico bestaat dat incidenten en afwijkingen in de verwerking van persoonsgegevens niet tijdig worden gedetecteerd, aangezien CEM geen gebruikmaakt van actieve monitoring of geautomatiseerde detectiesystemen. In de praktijk worden afwijkingen vooral opgemerkt via meldingen aan de supportdesk. Hierdoor is de kans aanwezig dat onregelmatigheden pas laat aan het licht komen, waardoor betrokkenen gedurende langere tijd risico lopen op verlies van BIV van hun persoonsgegevens, zonder dat zij hiervan op de hoogte worden gesteld of bescherming kunnen inroepen.	Gemiddeld	Hoog	Hoog
---	-----------	------	------

Het risico bestaat dat beveiligingsrisico's en kwetsbaarheden binnen CEM onvoldoende tijdig of volledig in beeld zijn, aangezien er geen structureel risicomanagementproces is ingericht. Risico-identificatie vindt vooral plaats op incidentele basis of wanneer er concrete aanleiding toe is. Hierdoor bestaat het risico dat bestaande dreigingen en zwakke plekken in systemen of processen onopgemerkt blijven, met als gevolg dat persoonsgegevens van betrokkenen in onvoldoende	Gemiddeld	Gemiddeld	Gemiddeld
---	-----------	-----------	-----------

beveiligde omgevingen worden verwerkt.

Het risico bestaat dat binnen Paragin medewerkers toegang hebben tot persoonsgegevens zonder dat dit noodzakelijk is voor de uitvoering van hun functie. Hoewel Paragin aangeeft passende beheersmaatregelen te hebben getroffen, is niet vastgesteld dat toegang tot persoonsgegevens strikt is ingericht op basis van rollen en 'need-to-know'. Dit verhoogt het risico dat persoonsgegevens van betrokkenen worden ingezien of verwerkt door onbevoegde medewerkers, wat kan leiden tot verlies van vertrouwelijkheid en een beperking van de controle die betrokkenen over hun gegevens hebben.	Laag	Hoog	Laag
---	------	------	------

6. Maatregelen en restrisico's

In dit hoofdstuk wordt beschreven welke maatregelen kunnen worden getroffen om de gesignaleerde risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen betreft een afweging van de verwerkingsverantwoordelijke en in enkele gevallen van de verwerker.

In onderstaande tabel zijn de geconstateerde risico's beschreven in het kader van de verwerking van persoonsgegevens door de CEM. Daarnaast is beoordeeld welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Per risico is beschreven welke maatregel welk risico aanpakt.

Voor de inschatting van de kans, impact en het risico zijn de niveaus 'laag', 'gemiddeld' en 'hoog' gebruikt. Het risico wordt bepaald aan de hand van de formule kans x impact.

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Het risico bestaat dat het overzicht van verwerkte persoonsgegevens (het verwerkingsregister) binnen de mbo-instelling niet up-to-date is. Dit kan leiden tot situaties waarin betrokkenen hun rechten niet kunnen uitoefenen, en tot het niet voldoen aan de verantwoordingsplicht die op mbo-instellingen als verwerkingsverantwoordelijke rust.	Mbo-instellingen dienen het verwerkingsregister bij te verwerken met alle verwerkingen die worden uitgevoerd door de CEM. Daarbij dient onder andere te worden uitgelegd welke persoonsgegevens worden verwerkt, hoelang de gegevens bewaard blijven en welke beveiligingsmaatregelen zijn getroffen.	Laag	Mbo-instelling
De CEM beschikt op dit moment niet over een verwerkingsregister waarin de verwerkingen, die worden uitgevoerd in de hoedanigheid van verwerker, zijn opgenomen. Dit kan leiden tot een gebrek aan inzicht in verwerkingen die worden uitgevoerd ten behoeve van de mbo-instellingen en verhoogde risico's op onrechtmatige of onveilige gegevensverwerking.	De CEM stelt zo spoedig mogelijk een volledig en actueel verwerkingsregister op waarin alle verwerkingen zijn opgenomen die namens de mbo-instellingen worden uitgevoerd in de hoedanigheid van verwerker. Dit register voldoet aan de eisen uit artikel 30 AVG en bevat ten minste: • de doeleinden van de verwerkingen; • een beschrijving van de categorieën van betrokkenen en persoonsgegevens; • de categorieën van ontvangers;	Laag	CEM

- eventuele doorgiften aan derde landen;
- beoogde termijnen voor het wissen van gegevens;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen door CEM niet vooraf door mbo-instellingen zelf zijn vastgelegd, eveneens in het verwerkingsregister. Dat zou leiden tot een onrechtmatige verwerking die ook de uitoefening door betrokkenen van hun rechten kan belemmeren.	Mbo-instellingen dienen zelf de verwerkingsdoeleinden vast te stellen en vast te leggen in het verwerkingsregister. Enkel benoeming van de (algemene) verwerkingsdoeleinden in deze DPIA volstaat niet voor het voldoen aan de verantwoordingsplicht.	Laag	Mbo-instelling
Binnen beide gegevensverwerkingen (het plannen/vaststellen en het afnemen/analyseren van (reken)examens) worden persoonsgegevens verwerkt die niet strikt noodzakelijk zijn voor het bereiken van het verwerkingsdoel. Het betreft hier onder meer de adresgegevens (adres, plaats, postcode, land) van medewerkers en studenten, alsook gezondheidsgegevens van studenten (zoals informatie over extra tijd of visuele beperkingen) die zichtbaar zijn in loggingfunctionaliteiten van Stipp. Verwerking van niet-noodzakelijke persoonsgegevens leidt tot een schending van het beginsel van dataminimalisatie zoals voorgeschreven door de AVG. Dit verhoogt het risico op datalekken en ongeoorloofde toegang tot gevoelige informatie, met mogelijke reputatieschade en juridische	De CEM dient een gegevensreductie door te voeren. Verwerk enkel de strikt noodzakelijke gegevens. Schakel de optionele velden (zoals adresgegevens) standaard uit tenzij expliciet gemotiveerd.	Laag	CEM

gevolgen voor de mbo-instelling.

Het risico bestaat dat persoonsgegevens langer worden bewaard dan noodzakelijk. Dat risico kan ontstaan doordat ofwel geen bewaartermijn is vastgesteld ofwel doordat bewaartermijnen niet consequent worden gehandhaafd. Dat leidt tot een onrechtmatige verwerking van persoonsgegevens en tot een groter risico bij beveiligingsincidenten.	De mbo-instelling dient de bewaartermijnen vast te stellen en vast te leggen. De mbo-instelling is zelf verantwoordelijk voor (geautomatiseerde) verwijdering. Wij adviseren de mbo-instellingen om geautomatiseerde verwijdering van reeds vastgestelde termijnen in te voeren. Paragin dient de opschoontermijn die standaard staat ingesteld op 'nooit' aan te passen, zodat de persoonsgegevens niet langer standaard oneindig bewaard worden.	Laag	Mbo-instelling
Het risico bestaat dat er geen passende afspraken zijn gemaakt met partijen door wie persoonsgegevens worden verwerkt. Als dit niet, niet tijdig, of niet correct wordt gedaan, ontstaat het risico dat de ontvangende partij de persoonsgegevens onbehoorlijk verwerkt. Dit leidt voor betrokkenen tot het risico op misbruik van persoonsgegevens, datalekken, verlies van vertrouwelijkheid, en dat betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen.	De mbo-instelling dient een verwerkersovereenkomst te sluiten met de CEM. De CEM dient daarnaast nog een verwerkersovereenkomst te sluiten met leverancier Stipp. In deze verwerkersovereenkomst, of op een andere wijze, dienen ook afspraken te worden gemaakt over de lijst waarin gegevens omtrent logging zijn opgenomen. Er dienen afspraken te worden gemaakt over het periodiek opschonen van deze persoonsgegevens (lijst).	Laag	Mbo-instelling en CEM
Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op de mbo-instellingen rust. Hierdoor kunnen betrokkenen niet verwachten en/of anticiperen op welke wijze de desbetreffende partijen met hun persoonsgegevens omgaan. Dit leidt ertoe dat betrokkenen hun rechten niet	De mbo-instelling dient betrokkenen te informeren over de verwerking van hun persoonsgegevens. Dit dient zij te doen door middel van de privacyverklaring voor studenten en door middel van de privacyverklaring voor medewerkers.	Laag	Mbo-instelling

of minder goed kunnen uitoefenen.			
Het risico bestaat dat persoonsgegevens bij CEM ongeautoriseerd toegankelijk zijn, doordat geen encryptie wordt toegepast op data-at-rest en data-in-transit. Hoewel op onderdelen gegevens worden geanonimiseerd, zijn andere gegevens onvoldoende beschermd bij een beveiligingsincident. Dit kan ertoe leiden dat persoonsgegevens van betrokkenen bij verlies of diefstal van gegevens ongewenst worden ingezien, wat schade kan veroorzaken aan hun privacy.	De CEM dient persoonsgegevens te beveiligen door versleuteling toe te passen op data-at-rest en data-in-transit. Dit dient zij te doen door het implementeren van encryptietechnieken conform actuele beveiligingsstandaarden (zoals AES-256 en TLS 1.2 of hoger) in alle systemen waarin persoonsgegevens worden verwerkt of opgeslagen.	Laag	CEM
Het risico bestaat dat incidenten en afwijkingen in de verwerking van persoonsgegevens niet tijdig worden gedetecteerd, aangezien CEM geen gebruikmaakt van actieve monitoring of geautomatiseerde detectiesystemen. In de praktijk worden afwijkingen vooral opgemerkt via meldingen aan de supportdesk. Hierdoor is de kans aanwezig dat onregelmatigheden pas laat aan het licht komen, waardoor betrokkenen gedurende langere tijd risico lopen op verlies van BIV van hun persoonsgegevens, zonder dat zij hiervan op de hoogte worden gesteld of bescherming kunnen inroepen.	De CEM dient incidenten en afwijkingen in de verwerking van persoonsgegevens tijdig te detecteren. Dit dient zij te doen door middel van actieve monitoring en het inzetten van geautomatiseerde detectiesystemen voor het signaleren van onregelmatigheden in gegevensverwerkingen.	Laag	CEM
Het risico bestaat dat beveiligingsrisico's en kwetsbaarheden binnen CEM onvoldoende tijdig of volledig in beeld zijn, aangezien er geen structureel risicomanagementproces is ingericht. Risico-identificatie	De CEM dient beveiligingsrisico's en kwetsbaarheden structureel in kaart te brengen. Dit dient zij te doen door middel van het inrichten en uitvoeren van een risicomanagementproces dat periodiek risico's identificeert, beoordeelt en mitigeert binnen	Laag	CEM

vindt vooral plaats op systemen en incidentele basis of wanneer verwerkingsprocessen. er concrete aanleiding toe is. Hierdoor bestaat het risico dat bestaande dreigingen en zwakke plekken in systemen of processen onopgemerkt blijven, met als gevolg dat persoonsgegevens van betrokkenen in onvoldoende beveiligde omgevingen worden verwerkt.

Het risico bestaat dat binnen Paragin medewerkers toegang hebben tot persoonsgegevens zonder dat dit noodzakelijk is voor de uitvoering van hun functie. Hoewel Paragin aangeeft passende beheersmaatregelen te hebben getroffen, is niet vastgesteld dat toegang tot persoonsgegevens strikt is ingericht op basis van rollen en 'need-to-know'. Dit verhoogt het risico dat persoonsgegevens van betrokkenen worden ingezien of verwerkt door onbevoegde medewerkers, wat kan leiden tot verlies van vertrouwelijkheid en een beperking van de controle die betrokkenen over hun gegevens hebben.	Paragin dient de toegang tot persoonsgegevens te beperken tot medewerkers voor wie dit noodzakelijk is. Dit dient zij te doen door middel van een strikt rol gebaseerd toegangsbeheer op basis van het 'need-to-know'-principe en door periodiek te controleren of de toegangsrechten aansluiten bij de functieverantwoordelijkheden.	Laag	Paragin
--	--	-------------	----------------

7. Ondertekening

Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	Erik Degen
Directie/afdeling verantwoordelijke(n)	Erik Degen
Functie verantwoordelijke(n)	Directeur
Datum ondertekening	11 juni 2025
Handtekening	