

DPIA CA

gegevensbeschermingseffectbeoordeling centraal aanmelden

Inhoudsopgave

A. AANLEIDING	4
B. VOORZIENING CENTRAAL AANMELDEN	4
C. MANagementsamenvatting	6
D. BESCHRIJVING KENMERKEN GEGEVENSVERWERKINGEN	8
Context	8
Relatie VVA en CA	9
Relatie met SIS	10
E. VRAGEN EN ANTWOORDEN MODEL DPIA RIJKSOVERHEID.....	10
1. Procesbeschrijving.....	10
2. Gegevens-elementen persoonsgegevens.....	12
3. Gegevensverwerkingen	14
4. Verwerkingsdoeleinden.....	15
5. Betrokken partijen	15
6. Belangen bij de gegevensverwerkingen.....	16
7. Verwerkingslocaties	17
8. Technieken en methoden van de gegevensverwerkingen	17
9. Juridisch en beleidsmatig kader.....	17
10. Bewaartermijnen.....	18
F. BEOORDELING RECHTMATIGHEID GEGEVENSVERWERKINGEN	19
11. Rechtsgrond/ grondslag	19
12. Bijzondere persoonsgegevens	20
13. Doelbinding	20
14. Noodzaak en evenredigheid	20
15. Rechten van de betrokkenen.....	21
G. BESCHRIJVING EN BEOORDELING RISICO'S EN MAATREGELEN.....	22
Ad 1. Berichten worden ten onrechte niet of te laat verzonden	26

Ad 2. Berichten worden op het verkeerde adres bezorgd.	26
Ad 3. Gegevens worden onbedoeld openbaar gemaakt.	27

H. CONCLUSIES EN AANBEVELINGEN..... 28

A. Aanleiding

Binnen de mbo-sector zijn vanaf 2016 activiteiten in gang gezet om te komen tot een voorziening die de instellingen ondersteunt bij de gegevenslevering die nodig is voor vroegtijdig aanmelden in combinatie met toelatingsrecht. Het eerste deel van deze plannen is gerealiseerd: de voorziening vroegtijdig aanmelden (VVA), het vervolg centraal aanmelden (CA) volgt per 1 december 2020. Aangezien het zowel bij VVA als CA om grootschalige verwerkingen van persoonsgegevens gaat, waarbij ook gevoelige persoonsgegevens worden verwerkt, is er in een eerdere fase een gegevensbeschermingseffectbeoordeling (hierna: DPIA of *data protection impact assessment*) voor VVA uitgevoerd en in dit document worden de bevindingen van de DPIA op CA gerapporteerd.

De scope van deze DPIA is de Voorziening Centraal Aanmelden (CA). Bij de DPIA is uitgegaan van het Programma van Eisen en documentatie (Audit Logius door Duinborgh, Analyse Compliance CA, verwerkersovereenkomst met bijlagen) CA. In deze DPIA is het proces van CA in de gehele keten geschetst. Het is belangrijk om hier te benadrukken dat deze DPIA uitsluitend betrekking heeft op de gegevensverwerking binnen de voorziening CA. Er is een separate DPIA VVA uitgevoerd. Er is geen technische audit of controle uitgevoerd op CA (zie de opmerking daaromtrent bij aanbevelingen). De DPIA is derhalve gebaseerd op de beschikbare documentatie en analyses.

De voorziening CA is een gezamenlijk initiatief van de mbo-instellingen, saMBO-ICT ondersteund door de MBO Raad. Dat maakt dat er een gemeenschappelijk belang is om ervoor te zorgen dat ook informatiebeveiliging en privacy goed geregeld zijn. In dat kader is er besloten om een DPIA uit te voeren. Deze DPIA is in oktober/ november 2020 uitgevoerd door Job Vos (Vos Juridisch Advies) met medewerking van Peter Vermeijs (MBO Raad), Martijn Bijleveld (saMBO-ICT) en Ymkje Koster (Kennisset).

B. Voorziening Centraal Aanmelden

Centraal Aanmelden mbo is een gezamenlijk portaal waarmee een nieuwe mbo-student zich kan aanmelden bij een mbo-instelling voor een opleiding. Dat kan door direct naar de website voor Centraal Aanmelden te gaan, of via een doorverwijzing vanuit de website van de mbo-instelling.

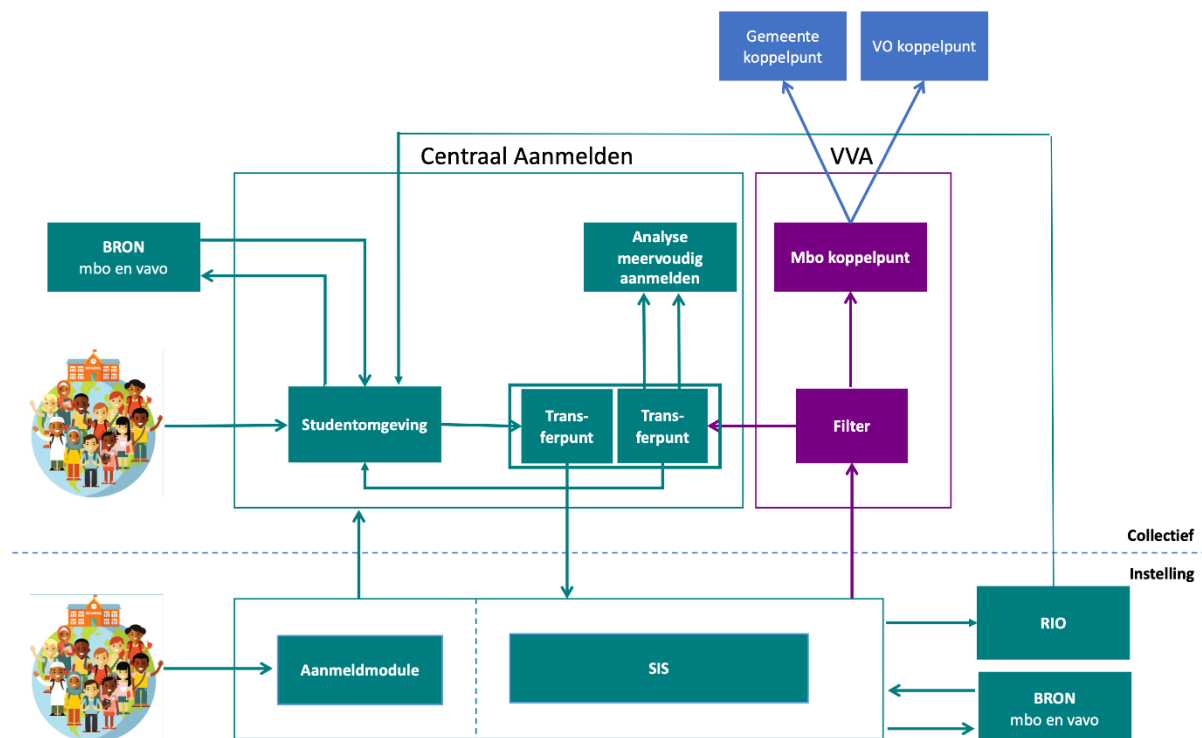
Het eerste wat het portaal regelt is de identificatie met DigiD (en in de toekomst e-ID met andere toegestane identificatiemiddelen). De student haalt na identificatie alle standaardgegevens (officiële persoonsgegevens en de vooropleiding-gegevens) op bij DUO en vult deze aan met eigen contactinformatie. Studenten zonder DigiD loggen in met gebruikersnaam en wachtwoord, waarna identificatie plaatsvindt via de mbo-instelling.

Vervolgens kan een student zich binnen de voorziening CA aanmelden bij een instelling en een opleiding. Dat mogen in de praktijk ook meerdere aanmeldingen zijn. Nadat de student een bevestiging ontvangt wordt het vervolg van het traject overgelaten aan de school. De instelling verzorgt de verdere communicatie en plaatsing.

Een analysetool geeft landelijk, overkoepelend inzicht in de aanmeldingenstromen. Daarnaast krijgen instellingen inzicht in aantallen (meervoudige) aanmeldingen voor hun eigen opleidingen. De informatie is gericht op inzicht voor instellingen ten behoeve van een efficiënte bedrijfsvoering.

Centraal Aanmelden in het mbo-sector is ontstaan vanuit een aantal behoeften vanuit de mbo-sector:

- Identificatie moet geregeld zijn
Van een aanmelding is alleen sprake wanneer de identificatie goed is geregeld. Dat zou elke instelling apart kunnen doen, maar de eisen die worden gesteld aan de inrichting van bijvoorbeeld DigiD zijn hoog en tijdrovend. Het is beter om dat gemeenschappelijk te doen, dat scheelt veel tijd en kosten.
- Aanmelden bij het mbo is uniform
Scholieren uit het voortgezet onderwijs dienen zich voor 1 april aan te melden bij het mbo. Een uniforme manier van aanmelden, maakt goede voorlichting mogelijk. De vraag 'hoe moet ik mij aanmelden bij een mbo-instelling' kan dan eenvoudig worden beantwoord.
- Noodzakelijk bij maximum aantallen aanmeldingen
De voorziening is noodzakelijk wanneer er sprake is van een maximum aantal aanmeldingen voor een bepaalde opleiding (numerus fixus). De mbo-instelling moet zicht houden op (mogelijke) aanmeldingen die kunnen leiden tot inschrijving.
- Aanmelden is een juridische status geworden
In combinatie met toelatingsrecht is een aanmelding, gekoppeld aan een datum van aanmelden, een status waaraan rechten ontleend kunnen worden. Dat stelt eisen aan een transparante en zuivere manier van aanmelden.
- Inzicht in meervoudige aanmeldingen
Elke inschrijving gaat gepaard met gemiddeld twee aanmeldingen. Centraal aanmelden levert de mbo-instellingen geanonimiseerd het inzicht dat onder andere nodig is voor goede prognoses en bedrijfsvoering.



C. Managementsamenvatting

Onderwijsinstellingen maken steeds beter en meer gebruik van ICT. Daardoor neemt het aantal persoonsgegevens dat scholen gebruiken toe. Het beschermen van de privacy van onderwijsdeelnemers en medewerkers wordt daarom steeds belangrijker. De besturen van deze onderwijsinstellingen zijn volgens de wet verplicht om privacy goed te regelen en beschermen. Er moeten goede en passende maatregelen worden genomen om deze persoonsgegevens te beschermen.

De Algemene Verordening Gegevensbescherming (AVG) verplicht organisaties zoals onderwijsinstellingen om te onderzoeken wat het effect is van het verwerken van persoonsgegevens op de privacy van (toekomstige) onderwijsdeelnemers en medewerkers. Dit onderzoek wordt gegevensbeschermingseffectbeoordeling genoemd. In Nederland wordt vaak de Engelse benaming gebruikt: Data Protection Impact Assessment of DPIA. Het is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen, om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Aan de hand van de DPIA wordt onderzocht wat het effect op de privacy van de betrokkenen is bij het verwerken van persoonsgegevens. De DPIA is een analyse van de kans dat een risico of bedreiging werkelijkheid wordt en wat de gevolgen hiervan zijn. Daarnaast wordt beschreven welke maatregelen genomen zijn en nog kunnen worden genomen om eventuele privacy schendingen te voorkomen. De DPIA geeft dus inzicht in de risico's die het verwerken van persoonsgegevens binnen de onderwijsinstelling oplevert.

Een DPIA is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de privacy van onderwijsdeelnemers en medewerkers. Het uitvoeren van een DPIA is bijvoorbeeld verplicht als het gaat om een grootschalige verwerking van persoonsgegevens.

In het mbo wordt vanaf 1 december 2020 gebruik gemaakt van de voorziening Centraal Aanmelden (CA). Deze voorziening wordt aangeboden door de Coöperatie MBO Voorzieningen U.A. Omdat deze voorziening bedoeld is om – op termijn - alle aanmeldingen van nieuwe studenten te gaan verwerken, is er sprake van een grootschalige verwerking van persoonsgegevens waar een DPIA voor moet worden uitgevoerd. Er is een DPIA uitgevoerd op de voorziening Centraal Aanmelden; in dit rapport worden de uitkomsten van de DPIA beschreven.

De conclusie van deze DPIA is dat de verwerking van persoonsgegevens van (aspirant-)studenten in de voorziening Centraal Aanmelden een **beperkt risico** inhoudt voor de rechten en vrijheden van deze aspirant-studenten. De risico's zijn laag tot gemiddeld. Op basis van de door de Coöperatie genomen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen binnen Centraal Aanmelden wordt de privacy (van de persoonsgegevens) van aspirant-studenten in voldoende mate gegarandeerd.

Er is niet gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moeten leiden tot een 'voorafgaande raadpleging' bij de privacy toezichthouder, de Autoriteit Persoonsgegevens (zoals omschreven in artikel 36 AVG).

Bij het uitvoeren van de DPIA is een aantal risico's geconstateerd die verder beperkt kunnen worden door extra te nemen maatregelen. Deze maatregelen en risico's zijn beschreven in hoofdstuk H (conclusies en aanbevelingen). De aanbevelingen zijn besproken met de Coöperatie MBO Voorzieningen, die deze aanbevelingen over zal nemen en implementeren de komende maanden.

Hiermee zijn risico's voor de rechten en vrijheden van aspirant-studenten in voldoende mate geadresseerd zodat - na uitvoering van de aanbevelingen - de betreffende producten en diensten van de voorziening Centraal Aanmelden conform de AVG kunnen worden gebruikt door mbo-instellingen.

De Colleges van Bestuur van mbo-instellingen zijn verplicht om zelf een DPIA uit te (laten) voeren. Om te voorkomen dat iedere mbo-instelling zelf een DPIA uit moet voeren, is sector breed het initiatief genomen tot deze DPIA. Deze DPIA kan als uitgangspunt dienen voor mbo-instellingen. Zij kunnen op basis van de DPIA een weloverwogen besluit te nemen om – al dan niet vooruitlopend op afronding van implementatie van de aanbevelingen – de voorziening Centraal Aanmelden te gaan gebruiken.

D. Beschrijving kenmerken gegevensverwerkingen

Context

De voorziening CA regelt het centraal aanmelden van aspirant-studenten in het mbo en deze voorziening hangt nauw samen met VVA; de 'Wet vroegtijdige aanmelddatum voor en toelatingsrecht tot het mbo' die op 1 augustus 2017 in werking is getreden. Dit leidt ertoe dat degenen die zich willen inschrijven bij een mbo, zich vóór 1 april bij de desbetreffende instelling moeten aanmelden. Daarnaast is er een plicht ontstaan voor de onderwijsinstellingen om een beperkte gegevensset over aanmeldingen met elkaar en met gemeenten uit te wisselen.

Het doel van de wet is om de overstap van jongeren naar het mbo goed te laten verlopen en daarbij de positie van de student te versterken. Een subdoel is om een sluitende informatievoorziening te creëren waarmee alle overstappende jongeren in Nederland met behulp van actuele informatie gedurende de overstap op de voet gevolgd en tijdig begeleid kunnen worden, zodat ze aankomen op het mbo. Dit draagt bij aan het voorkomen van voortijdig schoolverlaten (VSV).

Vo-scholen dienen aan te geven welke leerlingen naar verwachting een mbo-opleiding gaan volgen en de mbo-instellingen dienen de status van de aanmelding van deze leerlingen te melden aan de vo-scholen en in een aantal gevallen aan de gemeente, die daarmee in staat wordt gesteld om de wet leerplicht en wetgeving RMC te handhaven.

Om deze uitwisseling van gegevens te ondersteunen, is een informatiesysteem ontwikkeld: de Voorziening Vroegtijdig Aanmelden (VVA). Het mbo maakt gebruik van het koppelpunt mbo dat onderdeel is van de VVA. Dit proces is beschreven in de DPIA VVA.

Mbo-instellingen hebben daarnaast behoefte aan een uniform proces voor aspirant studenten die zich na identificatie kunnen inschrijven bij een mbo-opleiding. Hierbij staat de 'Wet vroegtijdige aanmelddatum voor en toelatingsrecht tot het mbo' centraal. Studenten worden, na identificatie via eID ingeschreven en hebben zelf inzage in de status van de voortgang van hun inschrijving dan wel aanmelding.

Omdat de aanmelding in het mbo een juridische status heeft gekregen, is ervoor gekozen om aanmelden centraal te organiseren. De datum van aanmelding (voor 1 april) geeft aspirant studenten immers een toelatingsrecht. Doordat het aanmelden centraal georganiseerd is, en beheerd wordt door een organisatie 'buiten' (buiten staat tussen haakjes want de Coöperatie MBO Voorzieningen U.A. is immers 100% eigendom van de instellingen) de onderwijsinstelling, hoeven instellingen hier niet ieder voor zich zorg voor te dragen en het proces (zoals rondom identificatie en authenticatie) in te regelen. De voorziening CA is 24/7 beschikbaar, waardoor het aanmeldproces voor aspirant studenten georganiseerd is. De voorziening geeft de student daarbij ook inzage in zijn aanmeldingsgegevens, waarmee tegemoet wordt gekomen aan het recht op inzage in het kader van de AVG.

Daarnaast bestaat bij instellingen de behoefte aan inzicht in meervoudige aanmeldingen: aspirant-studenten die zich bij meerdere opleidingen bij dezelfde instelling aanmelden en/of bij meerdere opleidingen van andere instellingen. Het gebrek aan inzicht zorgt op dit moment voor complexiteit in de capaciteitsplanning en bedrijfsvoering. Dat is een van de redenen waarom er behoefte is aan een voorziening voor CA. In de voorziening CA kan, met de gegevens van de aanmeldingen van aspirant-studenten (geanonimiseerd), een beeld worden opgebouwd van meervoudige aanmeldingen. Dit beeld kan vervolgens aan de instellingen beschikbaar worden gesteld ten behoeve van de capaciteitsplanning en de bedrijfsvoering.

De voorziening CA is een generieke voorziening, voorziening wordt dus niet instelling specifiek. Generiek gebruik, in het kader van gewenste uniformiteit, is van belang. De voorziening heeft een neutrale uitstraling namens het mbo. De voorziening kan worden gebruikt voor aanmelden voor mbo-opleidingen, VAVO-opleidingen (geen vakkenkeuze). Aanmelden voor vo-opleidingen, contractonderwijs, educatie en certificaatgericht onderwijs worden (nog) ondersteund.

Kortgezegd zijn de hoofddoelstellingen van CA:

- Centraal regelen van het aanmeldproces voor de studenten
 - Met de 'Wet vroegtijdig aanmelden en toelatingsrecht' krijgt aanmelden een formele status en de student toelatingsrecht
 - Student effectief en efficiënt ondersteunen bij aanmelden
 - Student tijdig en accuraat informeren over status aanmelding(en)
- Uniformeren van de aanmeldprocessen
 - Aanmelden op zelfde wijze en o.b.v. dezelfde informatie, bij iedere school
 - Bijdrage aan een effectief en efficiënt aanmeldproces
- Inzicht krijgen in meervoudige aanmeldingen op instelling en landelijk niveau
 - Verschil tussen aanmelding en inschrijving heeft invloed op bedrijfsvoering
 - CA kan inzicht geven, daarmee bedrijfsvoering optimaliseren

Relatie VVA en CA

De voorziening CA is zoals gemoed, onlosmakelijk verbonden met VVA. Om inzicht te krijgen in meervoudige aanmeldingen is het zelfs noodzakelijk dat de aanmeldinformatie uit het VVA-traject onderdeel uitmaakt van de CA-informatie. Om dit te bewerkstelligen is een zogenaamde "filterfunctie" ontworpen als onderdeel van de VVA-functionaliteit. Naast het filter bestaat de behoeftestelling VVA uit het 'koppelpunt mbo'. Bij de ontwikkeling van de behoeftestelling van VVA is ook al rekening gehouden met de voorziening CA, ten behoeve van een goede aansluiting. Daarom is de filterfunctie - die ervoor zorgt dat de juiste informatie van het studentinformatiesysteem (SIS) naar VVA wordt gestuurd - ondergebracht in de voorziening VVA. Het filter van VVA bepaalt welke gegevens doorgegeven worden aan CA, en welke informatie aan de voorgaande onderwijsinstelling en gemeente wordt doorgegeven. Doordat er een centraal filter is gerealiseerd, wordt voorkomen dat mbo-instellingen zelf dit koppelpunt (met bijbehorende gegevensuitwisseling) moeten realiseren binnen hun SIS.

Relatie met SIS

De voorziening CA heeft een relatie met de student informatiesystemen (SIS) van de instellingen en met VVA. De voor CA relevante functies van de SIS zijn de functiegebieden 'Aanmelden', 'Intake' en 'Kernregistratie'. Het gaat hierbij om wat binnen de voorziening CA wordt verzameld, dat voldoende moet zijn om te kunnen leiden naar 'Intake' en vervolgens 'Kernregistratie' ofwel een inschrijving. Hierbij worden de volgende processen onderscheiden:

- Inloggen met eID
- Persoonlijke studentomgeving inzien/wijzigen
- Intrekken aanmelding
- Persoonlijke studentomgeving opheffen
- Gegevens ophalen BRP en/of ROD
- Gegevens controleren/wijzigen/aanvullen
- Contactgegevens invullen
- Beheren aanbod en periode-informatie opleidingen
- Inzien en selecteren instellingen en opleidingen
- Bedrijfsgegevens invullen (BBL) (koppeling SBB white label)
- Controleren gegevens aanmelding
- Versturen aanmelding
- Inzien overzicht status(sen) aanmelding(en)
- Status aanmelding ontvangen
- Informatie uitwisselen met SIS.

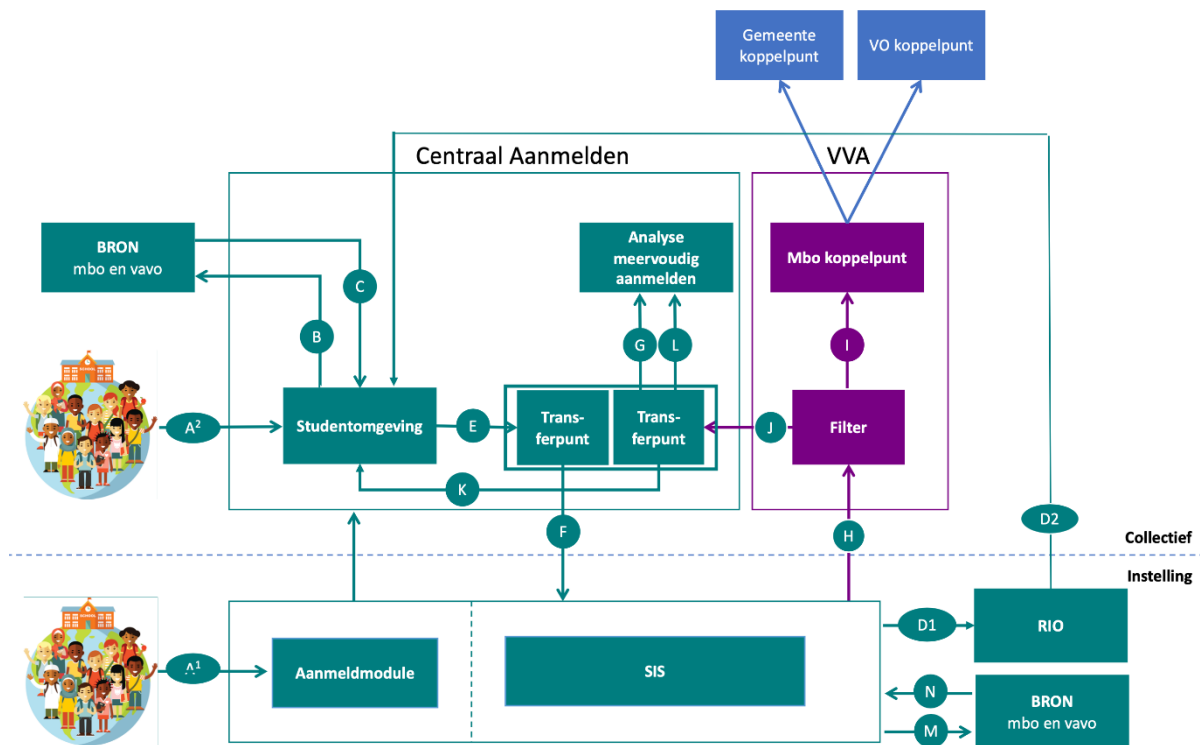
E. Vragen en antwoorden model DPIA Rijksoverheid

Voor deze DPIA is gebruikt gemaakt van het model gegevensbeschermingseffectbeoordeling Rijksdienst.

1. Procesbeschrijving

Het proces waar deze DPIA op ziet betreft de registratie en uitwisseling van persoonsgegevens en geanonimiseerde informatie van (toekomstig) mbo-studenten ten behoeve van hun aanmelding in het mbo.

In onderstaand schema wordt dit proces beschreven en uitgewerkt. In de figuur is tevens de relatie tussen VVA en de voorziening CA weergegeven. Daaronder zijn de functionaliteiten beschreven.



A. Aspirant-studenten die zich willen aanmelden voor een mbo-opleiding hebben 3 mogelijkheden:

A1 (1) direct via de instelling (als de instelling (nog) geen gebruik maakt van de voorziening CA). De instelling organiseert de identificatie van de aspirant-student zelf, óf

A2 (2) via de website, of een specifieke opleiding op de website, van de instelling. De aspirant-student wordt vanuit de instellingsomgeving doorgeleid naar de voorziening CA. De aspirant-student identificeert zich in CA met een eID (DIGID).

A2 (3) via de persoonlijke studentomgeving in de voorziening CA. De aspirant-student identificeert zich met een eID (DIGID).

B. Na identificatie worden persoonsgegevens (uit BRP) en gegevens over zijn/haar vooropleiding opgevraagd bij ROD.

C. Indien beschikbaar levert DUO op verzoek persoonsgegevens (uit BRP) en gegevens over de vooropleiding van de aspirant-student.

D.

D1 RIO wordt vanuit (een) schoolomgeving(en) gevuld met alle noodzakelijke gegevens ten behoeve van het opleidingsaanbod in de voorziening CA.

D2 Het opleidingsaanbod van de instelling in de voorziening CA wordt 24/7 geactualiseerd dankzij gegevensoverdracht uit het RIO-register. De relevante gegevens uit RIO worden opgeslagen in CA.

E. Alle (intrekken van) aanmeldingen vanuit de studentomgeving worden doorgestuurd naar het transferpunt.

F. Het transferpunt stuurt de (intrekken van) aanmeldingen door naar de betreffende instelling.

G. Het transferpunt stuurt alle mbo-aanmeldingen voor het 1e jaar van de opleiding vanuit de studentomgeving door naar anonimiseren.

- H.** Anonimiseren stuurt de geanonimiseerde gegevens door naar de analyse omgeving meervoudig aanmelden ten behoeve van de analyse en rapportage van meervoudig aanmelden.
- I.** De instelling verwerkt de aanmeldingen (aanmeldingen aan de poort én aanmeldingen die zij van de voorziening CA ontvangen) en voorziet deze in het verwerkingsproces van de afgesproken (VVA) statussen en stuurt ‘aanmeld- en statusberichten’ naar het filter.
- J.** Het filter filtert de statussen die zijn ontvangen van de instelling en zet relevante informatie door naar het VO-koppelpunt en het Gemeente-koppelpunt.
- K.** Het filter stuurt de status van de aanmelding door naar transferpunt
- L.** Het transferpunt stuurt de status van de aanmelding door naar de (persoonlijke) studentomgeving (indien beschikbaar), zodat deze ook zichtbaar wordt voor de aspirant-student.
- M.** Het transferpunt stuurt alle mbo-statusberichten (veranderingen) door naar anonimiseren.
- N.** Anonimiseren stuurt de geanonimiseerde gegevens door naar de analyse omgeving meervoudig aanmelden ten behoeve van de analyse en rapportage van meervoudig aanmelden.
- O.** De instelling wisselt informatie uit met BRON, zoals de inschrijving en het verkrijgen van een diploma.
- P.** BRON levert actuele persoons- en vooropleiding-gegevens aan de instelling.
Niet in beeld gebracht: na verloop van de bewaartermijn wordt de studentomgeving gewist.

Op hoofdlijn zijn de functionaliteiten:

- Het centraal aanmelden door aspirant-studenten bij opleidingen middels een persoonlijke studentomgeving, en uitwisselen van deze informatie met de onderwijsinstelling;
- Het transferpunt voor het routeren van aanmeldberichten aan de SIS van mbo-instellingen;
- Managementinformatie over de (meervoudige) aanmeldingen van aspirant-studenten (alleen mbo) door gegevens van alle aspirant-studentgegevens (van de geselecteerde doelgroepen) in/door de voorziening CA te registreren, wordt inzicht verkregen in (meervoudige) aanmeldingen in het mbo. Deze aanmeldgegevens (en statusberichten) worden (geanonimiseerd) gebruikt om analyses met betrekking tot (meervoudig) aanmelden te maken.

2. Gegevens-elementen persoonsgegevens

In het onderstaande overzicht is schematisch weergegeven welke categorieën persoonsgegevens verwerkt worden door en binnen CA. De gegevens worden in de studentomgeving van de student verwerkt.

Gegevens-elementen persoonsgegevens	DUO levert	Invoer door	Uit/via RIO		SBB. Uit:	VVA filter
	uit BRON	student		Uit/met SIS	stagemarkt. nl	
Aanmelding ID				X		X
CAKetenID				X		
Persoonsgebonden nummer ² : onderwijsnummer en BSN	X			X		X

Geslachtsnaam	x			x ³		
Voorletters	x			x ³		
Voornamen	x					
Roepnaam		x				
Geboortedatum	x			x		x
Geboorteplaats	x					
Geboorteland	x					
Geslacht	x			x ³		
Postcode	x			x		
Straatnaam	x					
Huisnummer	x			x		
Huisletter/toevoeging/aanduiding	x					
Locatie omschrijving	x					
Contactgegevens aspirant-student		x		x		
Wettelijk vertegenwoordiger + contactgegevens		x		x		
Cohort informatie			x			
Onderwijsaanbieder ID uit RIO van latende school*			x			x
Naam opleiding (incl. internationale benaming)			x			
BRIN ontvangende mbo-instelling				x		
Onderwijsaanbieder ID uit RIO ontvangende mbo-instelling			x	x		x
Onderwijsaanbieder, -locatie			x	x		x
Opleidingsprogramma			x			
Toelatingseisen J/N			x			
Status van de aanmelding (AO/OA/LNI/AI/LI)				x		x
Code vooropleiding				x		x
Afwijkende opleidingsduur			x	x		
Voorafgaande toestemming voor aanmelding noodzakelijk			x			
Periode (begin/einddatum)			x			
Startkwalificatie (J/N/O)				x		
Crebo			x	x		x
Leertraject (BOL/BBL/OVO/EX/ODT)			x	x		x
Datum overlijden	x					
Datum vertrek uit Nederland (emigratie)	x					
Indicatie geheim adres	x					
Buitenlands adres	x					
Naam en gegevens leerbedrijf		x			x	
Leerbedrijf id				x	x	
Contactpersoon erkenning (SBB)				x	x	
Tweede contactpersoon leerbedrijf		x		x		
Erkend leerbedrijf (j/n plus informatie erkenning)				x	x ⁴	

1: art. 8.0.3 lid 3 en 4 WEB

2: wettelijk identificatienummer

3: uitsluitend indien geen PGN kan worden aangeleverd

4: terugkoppeling vanuit stagemarkt.nl of het aangegeven/ingevoerde leerbedrijf erkend is, er worden geen persoonsgegevens uitgewisseld van de aspirant-student.

3. Gegevensverwerkingen

Aanmaken persoonlijke studentomgeving

Student logt in bij CA met e-ID (evt. via website opleiding) en identificeert zich daarmee bij CA. De student vult zijn contactgegevens in.

Studenten die niet over een BSN/PGN beschikken (geen e-ID hebben), maken een gebruikersnaam aan en voeren hun persoons-, adres-en contactgegevens in. Het wachtwoord wordt naar de e-mail van de student toegezonden. Omdat deze aspirant-student niet volgens de wettelijke eisen is geïdentificeerd en zijn persoons-en vooropleiding gegevens niet zijn gevalideerd betreft het een aanmelding zonder toelatingsrecht, vergelijkbaar met een 'interesse melding'. Na het doen van deze interessemelding bij een mbo-instelling, identificeert de student zich bij de onderwijsinstelling van de melding, meldt zich bij een mbo-instelling en identificeert zich daar.

Opheffen persoonlijke studentomgeving

De student kan zelf zijn persoonlijke studentomgeving opheffen, maar CA kan dat ook automatisch doen (vooral nog 365 dagen na de laatste wijziging in de persoonlijke studentomgeving). De gegevens worden na opheffing (aanmerken voor vernietiging) na 365 dagen vernietigd.

Verrijken persoonlijke studentomgeving

Door identificatie ontvangt DUO het BSN-nummer van de student. Op basis daarvan levert DUO via BRON de actuele persoons- en vooropleiding gegevens van de student aan het CA. Daarnaast levert BRON de actuele inschrijving en de VO-, MBO- en HO-diplomagegevens (inclusief cijfers indien beschikbaar) uit het basisregister onderwijs.

Wijzigen of aanvullen persoonlijke studentomgeving

De student dient de gegevens in de persoonlijke studentomgeving te controleren en kan deze wijzigen of aanvullen. BRP-gegevens en vooropleiding-gegevens die niet kloppen moet de student laten corrigeren via het BRP en BRON.

Vooropleiding-gegevens die niet in BRON staan (bijv. Buitenlandse diploma's) kan de student zelf aanvullen.

Beheren aanmeldingen voor opleidingen

De student die is ingelogd in de persoonlijke studentomgeving kan zich aanmelden voor een opleiding bij een bepaalde instelling. De gegevens over opleidingen en instellingen zijn afkomstig uit RIO. In de persoonlijke studentomgeving kan de student de status van zijn aanmelding zien. In de persoonlijke studentomgeving kan de student ook zijn aanmelding weer intrekken.

Als een student zich heeft aangemeld voor een BBL-opleiding kan hij de gegevens in de persoonlijke studentomgeving aanvullen met de bedrijfsgegevens van het leerbedrijf. Als het een erkend leerbedrijf betreft worden de gegevens door CA opgehaald uit het White Label van SBB. Als het om een niet-erkend leerbedrijf gaat vult de student, indien bekend, de bedrijfs- en contactgegevens zelf in.

Versturen aanmelding naar instelling

Na aanmelding en controle van de gegevens verstuurt de student de aanmelding via CA naar de SIS van de mbo-instelling. De instelling ontvangt de complete gegevensset uit de persoonlijke studentomgeving in het SIS. De student ontvangt een bevestigingsmail met tijdstempel van de aanmelding (van belang voor toelatingsrecht).

Anonimiseren aanmeldingen voor analyse meervoudig aanmelden

Het Transferpunt van het CA-systeem stuurt alle aanmeldingen voor het eerste jaar van de opleiding(en) vanuit de persoonlijke studentomgeving door naar de omgeving Anonimiseren van het CA-systeem, waar de gegevens worden geanonimiseerd. De geanonimiseerde gegevens worden doorgestuurd naar de analyse-omgeving meervoudig aanmelden ten behoeve van de analyse en rapportage van meervoudig aanmelden.

Doorsturen aanmeldstatus van SIS naar het CA-systeem via filter en transferpunt

Nadat de onderwijsinstelling de aanmelding heeft geregistreerd of de aanmelding verder verwerkt heeft, stuurt het SIS van de onderwijsinstelling automatisch een bericht naar het filter met status van de aanmelding. Dit bericht wordt automatisch gestuurd op de momenten dat het intake- of het welkomstproces van de aspirant-student één van de voorgedefinieerde statussen bereikt. Het filter stuurt de status door naar het transferpunt. Het transferpunt zorgt ervoor dat de statusberichten worden doorgezet naar de persoonlijke studentomgeving en naar anonimiseren die de informatie vervolgens doorstuurt naar de database t.b.v. analyse meervoudig aanmelden.

Doorsturen aanmeldgegevens en -status naar het MBO-koppelpunt via filter

Nadat de onderwijsinstelling de aanmelding heeft geregistreerd of de aanmelding verder verwerkt heeft, stuurt het SIS van de onderwijsinstelling automatisch een bericht naar het filter met status van de aanmelding. Dit bericht wordt automatisch gestuurd op de momenten dat het intake- of het welkomstproces van de aspirant-student één van de voorgedefinieerde statussen bereikt. Het filter ontvangt alle aanmeldberichten, filtert deze berichten zodat enkel de relevante berichten via het MBO-koppelpunt worden doorgestuurd naar het VO- en Gemeenten-koppelpunt in verband met VVA.

4. Verwerkingsdoeleinden

- Identificatie van aspirant-studenten
- Eenvormige en centrale wijze van aanmelden in het MBO
- Vastleggen exacte datum en tijd van aanmelding in verband met wettelijk toelatingsrecht
- Integere en complete gegevensset bij aanmelden
- Inzicht voor student in eigen gegevens en (status van) aanmeldingen
- Koppeling met VVA, zodat gegevens maar een keer hoeven te worden verzameld
- Inzicht in meervoudige aanmeldingen ten behoeve van de bedrijfsvoering van de instelling wat weer leidt tot efficiënte besteding van publieke middelen.

5. Betrokken partijen

Verwerkingsverantwoordelijke(n)

- Individuele mbo-instelling

- Gezamenlijke verwerkingsverantwoordelijken (het collectief van mbo-instellingen)

Verwerker

- leverancier SIS
- Voorziening CA: Coöperatie MBO Voorzieningen

Subverwerker

- leverancier voorziening CA (Topicus)

De voorziening CA is eigendom van de leden (scholen in het mbo-onderwijsveld) van de juridische entiteit Coöperatie MBO Voorzieningen u.a. en de doorontwikkeling en het beheer van de voorziening wordt uitgevoerd door de coöperatie. De onderwijsinstellingen bepalen het doel en middelen van de gegevensverwerkingen (art. 28 AVG) en moeten ingevolge art. 28 lid 3 en 9 AVG een verwerkersovereenkomst afsluiten met de coöperatie. De onderwijsinstellingen laten de Coöperatie namens hen de persoonsgegevens verwerken. Dit houdt in dat de Coöperatie een verwerker is en er met iedere onderwijsinstelling een verwerkersovereenkomst moet worden afgesloten.

Voor individuele aspirant-studenten die zijn ingelogd binnen CA en een keuze voor een mbo-instelling hebben gemaakt, maar wiens aanmelding nog niet worden doorgestuurd naar de SIS, is de dienst CA van Coöperatie MBO Voorzieningen verwerker voor de betreffende vmbo-onderwijsinstelling die verwerkingsverantwoordelijke is.

Voor individuele aspirant-studenten voor wie wél een studentenomgeving is aangemaakt in CA, en er binnen CA wel gegevens worden opgeslagen, maar waarbij de student geen (voorlopige) keuze voor een mbo-instelling heeft gemaakt (er is sprake van een niet-voltooid aanmelding), zijn de mbo-instellingen gezamenlijk verwerkingsverantwoordelijke. Er is immers door de student geen keuze gemaakt voor een mbo-instelling. Dit uitgangspunt wordt niet als zodanig beschreven in de documentatie. Het advies is om dit goed in de (verwerkers)overeenkomst mee te nemen zodat mbo-instellingen zich goed bewust zijn van hun verantwoordelijkheden. Na het aanmelden door de aspirant-student bij CA, wordt een 'dossier' aangemaakt en informatie opgehaald bij verschillende derden (zie hiervoor onderdeel 3). Deze informatie wordt opgeslagen in CA. Er is voor die informatie geen specifieke mbo-instelling aan te wijzen. CA is in dat geval verwerker voor alle mbo-instellingen aangesloten bij CA.

6. Belangen bij de gegevensverwerkingen

De verwerkingsverantwoordelijke heeft de volgende belangen bij de voorgenomen gegevensverwerkingen.

1. Identificatie van aspirant-studenten
2. Eenvormige wijze van aanmelden in het MBO
3. Vastleggen exacte datum en tijd van aanmelding in verband met toelatingsrecht
4. Integere en complete gegevensset bij aanmelden
5. Inzicht voor student in eigen gegevens en (status van) aanmeldingen
6. Koppeling met VVA, zodat gegevens - via VVA - maar een keer hoeven te worden uitgewisseld;
7. Inzicht in meervoudige aanmeldingen ten behoeve van de bedrijfsvoering van de instelling wat weer leidt tot efficiënte besteding van publieke middelen

7. Verwerkingslocaties

Onderwijsinstellingen: Nederland

Verwerkers: Coöperatie MBO Voorzieningen (Nederland), SIS* (EER)

Subverwerker: Topicus (EER)

** Onderwijsinstellingen dienen zelf te controleren of hun SIS-leverancier binnen de Europese Economische Ruimte de gegevens verwerkt.*

8. Technieken en methoden van de gegevensverwerkingen

De uitwisseling van gegevens geschiedt op basis van webservices, waarbij op berichtniveau wordt uitgewisseld. Hierbij gebruik o.a. gemaakt van de Edukoppeling-standaard en REST-protocol.

Edukoppeling schrijft voor hoe onderwijsinstellingen, uitvoeringsorganisaties en andere ketenpartijen gegevensuitwisselingen moeten opzetten. Deze standaard is afgeleid van Digikoppeling, die voor hetzelfde doel wordt gebruikt in de overheidswereld. Beide standaarden gaan over de communicatielaag voor de afhandeling van berichten (het transport) en niet over de inhoud van berichten. Met deze standaarden kunnen organisaties in het onderwijs (zoals onderwijsinstellingen, DUO, uitgevers, leveranciers van administratiepakketten en de Onderwijsinspectie) op een eenduidige manier (vertrouwelijke) gegevens met elkaar uitwisselen. Edukoppeling en Digikoppeling worden gebruikt voor de gegevensuitwisseling. Gebruikmaken van deze standaarden draagt in het algemeen bij aan de betrouwbaarheid en onderhoudbaarheid van de educatieve keten. Voor de beveiliging wordt op transportniveau gebruikgemaakt van TLS en op berichtniveau wordt WS Security toegepast, conform Edukoppeling (Digikoppeling). Op die manier wordt end-to-end beveiliging gerealiseerd wat bijdraagt aan een veilige gegevensuitwisseling.

De passende en technische en organisatorische maatregelen (art. 28 lid 1 AVG) zijn verder beschreven in bijlage 2 van de verwerkersovereenkomst. Deze maatregelen zijn gebaseerd op de BIV-classificatie behorend bij het in de onderwijssector gehanteerde standaard voor informatiebeveiliging (Certificeringsschema). Periodiek of bij grote wijzigingen/updates vindt er – bijvoorbeeld via een risicoworkshop – een analyse plaats van de grootste risico's op het gebied van informatiebeveiliging en privacy voor de voorziening CA. Hiermee worden risico's geïdentificeerd en gemitigeerd waarmee de beveiligingsmaatregelen 'passend' blijven.

9. Juridisch en beleidsmatig kader

Op de voorgenomen gegevensverwerkingen is, naast de AVG en UAVG, de hieronder genoemde wet- en regelgeving van toepassing:

- Art 2.5.5a Wet educatie en beroepsonderwijs
- Art 8.0.1 Wet educatie en beroepsonderwijs
- Art 8.0.2 Wet educatie en beroepsonderwijs
- Art 8.0.3 Wet educatie en beroepsonderwijs
- Art 8.1.1c Wet educatie en beroepsonderwijs
- Art 27d Wet op het voortgezet onderwijs

- Art 103b Wet op het voortgezet onderwijs
- Art. 42b Wet op de expertisecentra
- Regeling gegevensverstrekking bij overstap naar het mbo
- Wet sterk beroepsonderwijs (wijziging van de WEB)
- Oprichting en statuten Coöperatie MBO Voorzieningen
- Eerste verkenning centraal aanmelden (februari 2018).

10. Bewaartermijnen

Voor wat betreft het verwijderen, worden de gegevens niet direct verwijderd, maar gemarkeerd voor verwijderen en vervolgens in een nachtelijke 'job' daarna daadwerkelijk verwijderd. Dit geeft de student ook tijdelijk de mogelijkheid om het verwijderen ongedaan te maken. De gegevens worden op dat moment echt verwijderd.

De student kan zelf zijn 'profiel verwijderen' (bij menu optie 'Profiel'), of dit kan geautomatiseerd gebeuren na een vastgestelde periode, met een vooraankondiging en bevestiging aan de student (via email) nadat een persoonlijke studentomgeving is aangemaakt waar nooit een aanmelding mee is gedaan.

Een aspirant-student die na inloggen in CA geen keuze voor een opleiding en mbo-instelling heeft gemaakt, krijgt na 3 maanden een e-mail dat diens 'profiel' wordt verwijderd. In geval van een voltooide aanmelding en inschrijving, worden het 'profiel' en de gegevens van de aspirant-student gedurende één jaar bewaard waarna de student per e-mail een melding krijgt dat dienst 'profiel' wordt verwijderd.

Het moment waarop deze termijnen gaan lopen is niet gedefinieerd, dit wordt nog gespecificeerd.

Voor wat betreft de geanonimiseerde gegevens ten behoeve van meervoudig aanmelden, geldt dat op het moment dat persoonsgegevens onomkeerbaar onherkenbaar zijn gemaakt, deze niet meer onder de AVG vallen. In feite is het niet nodig voor deze informatie een bewaartermijn te specificeren. Uit het oogpunt van transparantie in de richting van de betrokkenen valt niettemin te adviseren wel een dergelijke termijn op te nemen in het vereiste Documentair Structuurplan (DSP). Er is geen termijn bepaald.

F. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond/ grondslag

De voorziening CA regelt het centraal aanmelden van aspirant-studenten in het mbo en deze voorziening hangt nauw samen met VVA. CA ondersteunt daarmee het centraal aanmelden en de berichtuitwisseling van mbo-instellingen rondom de status van aanmelding en inschrijving van aspirant-studenten. Deze berichtuitwisseling vindt plaats op basis van een wettelijke verplichting (Wet invoering van een vroegtijdige aanmelddatum voor en toelatingsrecht tot het beroepsonderwijs). Het filter van het koppelpunt bepaalt of en welk bericht wordt doorgezonden. De gegevens uit het SIS worden mede ten behoeve van dit filter uitgewisseld met het koppelpunt. Door het filter wordt privacy by design geïmplementeerd, doordat wordt gecontroleerd of het uitwisselen van het bericht voldoet aan de wettelijke eisen (dataminimalisatie). Een bericht wordt slechts verzonden als het aan de in de wet genoemde criteria voldoet en de ontvangen en verzonden berichten worden standaard verwijderd, wat voldoet aan het beginsel van privacy-by-default.

De uitwisseling tussen het SIS van de mbo-instelling met het mbo-koppelpunt, vindt hiernaast plaats op grond van de overeenkomst voor Centraal Aanmelden. Het inrichten van Centraal Aanmelden in de mbo-sector, betreft de keuze van de leden van de MBO Raad om deze voorziening in het mbo centraal in te richten. Daarmee wordt tevens invulling gegeven aan een taak van algemeen/publiek belang. Alle bestuurders van de mbo-instellingen hebben ingestemd met het inrichten van deze centrale voorziening, die door de Coöperatie wordt aangeboden. Bij deze besluitvorming is de keuze gemaakt dat een bericht van aanmelding van een nieuwe dan wel toekomstige mbo-ganger, bij iedere in de wet genoemde statuswijziging wordt doorgegeven aan het koppelpunt mbo (dat op basis van het filter bepaalt of het bericht naar de koppelpunten vo/gemeente en de voorziening CA moet gaan). De keuze voor een voorziening Centraal Aanmelden is mede ingegeven door de wens om de keuzevrijheid van de studenten te vergroten, het aanmeldproces eenduidig te maken en daarmee te vereenvoudigen en de student te ondersteunen in zijn (studie)keuzeprocess. Hierdoor wordt op verantwoorde wijze invulling gegeven aan het toelatingsrecht van de onderwijsdeelnemer.

De voorziening CA is mede gericht op samenwerking tussen mbo-instellingen, reden waarom de Coöperatie MBO Voorzieningen - blijkens haar statuten - is opgericht met als doel te voorzien in een het ontwikkelen en beheren van voorzieningen en de bijbehorende dienstverlening ten behoeve van het middelbaar beroepsonderwijs in Nederland.

De grondslag voor het gebruik van de voorziening CA is daarmee uitvoering geven aan het toelatingsrecht: dit is een wettelijke taak. Nu staat daar tegenover dat de WEB geen verplichting kent om aanmelding en inschrijvingen centraal te laten verlopen. Het centraal inrichten van een aanmeldvoorziening in het mbo ligt daarnaast in het verlengde van het algemeen belang/publieke taak.

Met betrekking tot met name gegevens rondom meervoudig aanmelden, geldt dat CA voorziet in het doelmatig besteden van publieke middelen. Het inzicht in meervoudige

aanmeldingen is weliswaar omschreven als ten behoeve van de bedrijfsvoering van de instelling, maar het ziet daarmee op het efficiënt omgaan met publiek geld. Dit is een taak van eenieder: een taak van algemeen belang dan wel een publiek taak.

Voor het mbo geldt voorts dat - tot het moment dat de OOK wordt afgeschaft - de informatie-uitwisseling die plaatsvindt, te kwalificeren is als gegevensuitwisseling in en ten behoeve van de precontractuele fase. Mogelijk dat de wetgeving meer helderheid zal geven over de grondslag.

Nadrukkelijk is overwogen dat toestemming hiervoor géén grondslag is nu de aspirant-student verplicht is een set met gegevens te verstrekken bij aanmelding en inschrijving.

12. Bijzondere persoonsgegevens

Bij verwerking wordt gebruikgemaakt van een wettelijk identificatienummer (PGN); het gebruik hiervan is voorgeschreven in de Wet vroegtijdige aanmelddatum en toelatingsrecht tot het mbo. Het gebruik van het PGN bij aanmelding en inschrijving is voorgeschreven in de Wet voortgezet onderwijs en de Wet educaties en beroepsonderwijs. Daarmee is het gebruik van het PGN wettelijk geregeld en voldoet het aan de uitgangspunten van artikel 46 UAVG.

Bij het inloggen met DigiD krijgt CA direct een geverifieerd BSN, waarmee CA de potentiële student uniek heeft geïdentificeerd en geauthenticeerd. Hiermee wordt zekerheid geleverd met betrekking tot de identiteit van de student.

13. Doelbinding

De hiervoor omschreven persoonsgegevens worden verwerkt in dit wettelijke kader: versterken positie aspirant-student bij aanmelding en inschrijving, de voorziening CA regelt het toelatingsrecht.

De verwerkersovereenkomst geeft invulling aan het doelbinding-beginsel voor de Coöperatie MBO Voorzieningen.

14. Noodzaak en evenredigheid

Bij de noodzaak en evenredigheid geldt dat de wetgever een afweging heeft gemaakt over de door de onderwijsinstellingen en aspirant-student uit te wisselen informatie. Daar zit geen keuzevrijheid voor onderwijsinstellingen en aspirant-student. De afwegingsvrijheid voor onderwijsinstelling welke gegevens moeten worden gevraagd en uitgewisseld, is omschreven in de WEB. Ook het uitwisselen van de statuswijziging voldoet aan de wettelijke criteria en daarmee doorgegeven moet worden aan de (va)vo-school en/of gemeente.

Proportionaliteit

De verwerking van persoonsgegevens van aspirant-studenten in de voorziening Centraal Aanmelden is proportioneel. Er wordt uitvoering gegeven aan een wettelijke taak (toelatingsrecht), gegevens worden centraal ingevoerd en geverifieerd. Dit heeft als voordeel dat gegevens op één plek geregistreerd zijn en integer zijn (in plaats dat iedere

instelling zelf gegevens verzamelt en zelf moet zorgdragen voor de integriteit van deze data). Het biedt studenten rechtszekerheid omtrent hun toelatingsrecht nu er centraal, onafhankelijk van de mbo-instelling, een registratie van de aanmelding plaatsvindt. Het is daarnaast kostenbesparend vanwege een efficiënte besteding van publieke middelen. Er worden niet meer persoonsgegevens verzameld dan nodig in het kader van de aanmelding (en vervolgens: inschrijving). Daarnaast is CA gekoppeld met VVA waardoor de wettelijke uitwisseling van statussen van aanmelding en inschrijving centraal geregeld blijft en daarmee het vroegtijdig schoolverlaten terugdringt.

Subsidiariteit

Deze oplossing is de minst invasieve methode omdat de aspirant-student zich aanmeldt bij CA en daarmee niet onderworpen is aan eventuele aanvullende eisen vanuit mbo-instellingen met betrekking tot aanmelding. Gegevens zijn daarmee beschikbaar voor meerdere aanmeldingen bij verschillende mbo-instellingen zonder dat de aspirant-student diens gegevens opnieuw moet invoeren. Er worden niet meer gegevens gevraagd dan nodig, uitwisseling van deze gegevens geschiedt éénmalig en op veilige wijze via CA.

15. Rechten van de betrokkenen

Voor de uitwisseling van gegevens van de voorziening CA zijn alle bij de Coöperatie aangesloten onderwijsinstellingen gezamenlijke verwerkingsverantwoordelijke. De onderwijsdeelnemers kunnen bij deze Coöperatie 'rechten van betrokkenen' uitoefenen. De Coöperatie treedt op richting de aspirant-studenten als aanspreekpunt.

Omdat de voorziening CA en het SIS een verwerker zijn van de onderwijsinstellingen, kan de mbo-instelling alle rechten van de betrokkenen garanderen (mits de instelling de uitoefening van deze rechten zelf intern goed heeft georganiseerd). Uit het PvE CA zijn geen belemmeringen daarvoor gebleken. Er is overigens niet gebleken van een print- of exportmogelijkheid van data uit CA (los van de voorziene uitwisselingen tussen CA en mbo-instellingen).

Leerlingen die zich aanmelden worden door de voorziening CA (via het studentendossier in CA) geïnformeerd over de uitwisseling van de status van de aanmelding en de levering van persoonsgegevens. Het informeren van de betrokkenen is noodzakelijk op grond van artikel 13 AVG (te verstrekken informatie wanneer persoons- gegevens bij de betrokkene worden verzameld). Het verdient aanbeveling om binnen CA aspirant-studenten te informeren over hun rechten. Er is een privacyreglement in ontwikkeling (beoogde oplevering voor 1 december 2020).

De onderwijsinstelling heeft verwerkersovereenkomsten met de Coöperatie MBO Voorzieningen (CA), de leverancier van het SIS (VVA mbo-koppelpunt). Iedere individuele onderwijsinstelling zal op basis van deze verwerking het verwerkingenregister (moeten) aanpassen.

G. Beschrijving en beoordeling risico's en maatregelen

Op basis van de hiervoor genoemde feiten en omstandigheden, worden de volgende te noemen risico's geïdentificeerd en benoemd, waarop mogelijke mitigerende maatregelen beschreven zijn waarna een eventueel restrisico wordt benoemd. Risico's worden afgewogen op basis van 'kans * impact'.

Risico's met betrekking tot de rolverdeling (verantwoordelijke/verwerker)

Onderwijsinstellingen zijn zelfstandig verwerkingsverantwoordelijke met betrekking tot de gegevens die door CA met hen worden uitgewisseld. In deze DPIA is de conclusie dat onvoldoende gerealiseerd is wie verantwoordelijk is voor de data van aspirant-studenten voordat zij zich aanmelden bij een mbo-instelling. Voor deze student-gegevens zijn de mbo-instellingen die gebruik maken van CA aan te wijzen als gezamenlijk verwerkingsverantwoordelijken.

Risico's zijn hierbij dat in geval van incidenten en calamiteiten de rolverdeling tussen de mbo-instellingen en de Coöperatie MBO Voorzieningen U.A. niet voldoende inzichtelijk zijn, en dat incidenten en eventuele datalekken niet op de juiste wijze worden afgehandeld. Terwijl processen binnen de Coöperatie MBO Voorzieningen U.A. hieromtrent geregeld zijn, is communicatie over de rolverdeling niet even helder beschreven richting mbo-instellingen die gebruik maken van CA. Het risico blijft daarmee dat wettelijk verplichte meldingen niet, onjuist of te laat worden gedaan. Dit risico wordt beoordeeld als gemiddeld.

Maatregelen die genomen kunnen worden om dit risico te mitigeren, zijn het aanpassen van de verwerkersovereenkomsten op dit punt, alsmede het maken van afspraken tussen de mbo-instellingen die gebruik maken van CA, en het bestuur van de Coöperatie. Deze afspraken over de rolverdeling zijn nu niet of onvoldoende beschreven, we bevelen daarom aan dat de Coöperatie hierover in gesprek gaat met haar leden. Een 'regeling gezamenlijke verwerkingsverantwoordelijken' als onderdeel in de verwerkersovereenkomst behoort tot de opties. Ook zal de Coöperatie afspraken moeten maken of communiceren over de procedures in geval van incidenten en datalekken.

Hiernaast moet deze rolverdeling helder worden uitgelegd aan de betrokkenen, bijvoorbeeld via uitleg, FAQ en privacyreglement. In de documentatie is daar weinig informatie over aangetroffen, bij navraag blijkt dat informatie beschikbaar is of zal komen voor (aspirant)studenten. Het verdient aanbeveling om in de voorziening zelf informatie voor aspirant-studenten op te nemen over privacy, op en voor hen begrijpelijk taalniveau. Het beschikbaar stellen van een privacyreglement is niet voldoende. Dit risico wordt beoordeeld als gemiddeld: het informeren van betrokkenen is een wettelijke verplichting op grond van de AVG. Het verdient aanbeveling deze uitgangspunten van transparantie en informatievoorziening voor (aspirant-)studenten op te nemen in de documentatie.

Risico's met betrekking tot het bewaren van gegevens

In het kader van de DPIA is gebleken dat er weliswaar wordt gesproken over het bewaren van gegevens (zoals de studentgegevens in CA), maar dat concrete termijnen of afspraken over verwijdering/vernietiging van gegevens niet voldoende concreet zijn of ontbreken. Dit betekent dat het risico is dat persoonsgegevens onevenredig lang of langer dan noodzakelijk

worden verwerkt voor het doel waarvoor zij zijn verzameld. Het risico hierop wordt beoordeeld als gemiddeld. De aanbeveling is om binnen de Coöperatie afspraken te maken en vast te leggen omtrent bewaartermijnen, en deze informatie mede te delen met de betrokkenen.

Uit gesprekken met de Coöperatie MBO Voorzieningen, blijkt dat gegevens van een aspirant-student die wél is ingelogd maar zich niet heeft aangemeld (geen keuze heeft gemaakt voor een mbo-instelling of opleiding), na drie maanden zullen worden verwijderd. Gegevens van een aspirant-student bij wie een succesvolle aanmelding heeft plaatsgevonden en een inschrijving heeft plaatsgevonden, worden na een jaar verwijderd. Voorafgaand aan verwijdering krijgt de aspirant-student een e-mail daarover. Deze informatie zal worden verwerkt in de documentatie van de voorziening CA en opgenomen in een door de Coöperatie MBO Voorzieningen U.A. te hanteren bewaarbeleid.

Ten aanzien van de geanonimiseerde gegevens met betrekking tot meervoudig aanmelden, geldt dat deze data strikt genomen niet onder het bereik van de AVG valt. Desalniettemin is opgevallen dat er geen afspraken lijken te zijn over het bewaren van deze data. In het kader van informatiemanagement en het DSP is dit wel aan te bevelen.

Risico's met betrekking tot integriteit en volledigheid van persoonsgegevens

Uit het PvE CA blijkt dat de gegevens van de aspirant-student binnen CA, bij aanmelding bij één of meerdere mbo-instellingen eenmalig worden uitgewisseld. Dit levert verschillende risico's op.

Wijzigingen in de contactgegevens van de student in CA worden niet doorgegeven aan de mbo-instelling, waardoor de gegevens bij de mbo-instelling niet langer actueel zijn. Het is aan de mbo-instelling om zelf te zorgen dat de gegevens van de aspirant-student actueel blijven, en om daarover te communiceren met de aspirant-student. De aspirant-student moet alle mbo-instellingen zelf informeren over wijzigingen.

Wijzigingen in de contactgegevens in CA zijn wel zichtbaar in CA, en worden doorgegeven naar een nieuwe mbo-instelling, als de aspirant-student zich voor die nieuwe opleiding aanmeldt. De vorige mbo-instelling krijgt deze gewijzigde contactgegevens niet.

De aspirant-student krijgt bij wijziging van zijn contactgegevens in CA een notificatie (pop-up venster) dat hij zelf de wijzigingen moet doorgeven. Indien alle contactgegevens niet juist blijken te zijn, dan kan de mbo-instelling (waarbij de aspirant-student zich heeft aangemeld) in ieder geval contact opnemen met de latende onderwijsinstelling aangezien deze informatie wél is aangeleverd. Mbo-instellingen zijn op de hoogte van deze functionaliteit.

De aspirant-student kan eventueel nadelige gevolgen ondervinden als diens contactgegevens verouderd zijn. Zo kan een uitnodiging van een intake naar de verkeerde of oude contactgegevens van de aspirant-student worden verzonden. Het risico wordt ingeschat op gemiddeld omdat gegevens mogelijk niet actueel, integer en juist zijn (wat een risico oplevert in het kader van de beschikbaarheid, integriteit en vertrouwelijkheid).

Een alternatieve maatregel om dit risico te mitigeren is dat CA het wijzigen van deze contactgegevens niet meer mogelijk maakt (na aanmelding), of dat CA alsnog voorziet in een bericht over deze wijziging aan de mbo-instellingen die het betreft. De aanbeveling is dat naast betrokkenen ook mbo-instellingen hier goed over worden geïnformeerd.

Een ander risico gaat over het verwijderen van gegevens van de aspirant-student in de SIS van de mbo-instelling. Als de aspirant-student zijn aanmelding intrekt, wordt deze wijziging – in het kader van VVA – doorgegeven aan de mbo-instelling. Deze wijziging wordt via een bericht doorgegeven aan de SIS. Op welke wijze dit bericht wordt verwerkt in de SIS, is niet bekend: is menselijke tussenkomst vereist, wordt het dossier van de aspirant-student ‘geflagd’ of wordt het dossier vernietigd? Het beleid van de mbo-instelling rondom het al dan niet verwijderen van gegevens van deze aspirant-student valt buiten scope van CA en dus van deze DPIA, maar er dient hier wel aandacht voor te zijn in het kader van de privacybescherming van de aspirant-student. Informatie hierover ontbreekt.

Risico's met betrekking tot geanonimiseerde gegevens in het kader van meervoudig aanmelden

De analyses voor Meervoudig Aanmelden vallen onder AVG Art. 89 betreffende statistische verwerking, aangezien het PGN in de broninformatie is opgenomen. Volgens AVG Overweging (162) moet worden geborgd dat het statistisch resultaat en de onderliggende persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen. Dit is een aandachtspunt bij het ontwerp, waarbij moet worden geborgd dat er geen identificeerbaarheid mogelijk is aan de uitvoerkant. Het risico bestaat dat data, gecombineerd met gegevens over opleiding, toch specifiek genoeg zal zijn om individuele aspirant-studenten te identificeren. Een meervoudige aanmelding bij een unieke beroepsopleiding maakt dat ook anonieme gegevens sneller herleidbaar zijn. Als het kan mogelijk is dat de populatie dusdanig klein is dat de betrokkene identificeerbaar kan worden, dan moeten hier aanvullende maatregelen worden genomen.

De standaard bij anonimiseren is bijvoorbeeld dat gegevens van personen ($n < 5$) niet worden getoond. Uit navraag blijkt dat deze maatregel technisch is geïmplementeerd in het dashboard voor de scholen binnen CA. We hebben deze maatregel niet teruggevonden in de documentatie.

Aangezien de geaggregeerde informatie alleen wordt teruggekoppeld aan de instelling waar de aanmelding heeft plaatsgevonden, lijkt dit een beperkt risico voor de betrokkene op te leveren. Mogelijk kunnen hierover aanvullende afspraken worden opgenomen in de documentatie, en zou dit eveneens moeten worden gecommuniceerd door de Coöperatie met de mbo-instellingen.

Risico's met betrekking tot beveiliging en techniek:

Op basis van art. 28, lid 3, onder h AVG, kan worden afgesproken dat de verwerker de genomen beveiligingsmaatregelen aantoont door middel van bijvoorbeeld audits en inspecties.

In het kader van deze DPIA heeft er geen technisch onderzoek of audit plaatsgevonden. Vanwege het aansluiten van de voorziening CA op DigiD, is er wel een DigiD beveiligingsassessment. Dit assessment is gebaseerd op regelgeving van de NOREA voor kwaliteitsbeheersing en een selectie van de beveiligingsrichtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het Nationaal Cyber Security Centrum. Er zijn bij deze assurance-opdracht geen bijzonderheden geconstateerd.

Omdat de voorziening CA een grootschalige verwerking van persoonsgegevens betreft, verdient het aanbeveling om op termijn van enkele maanden een onafhankelijke technische audit of inspectie te laten uitvoeren, en de uitkomsten hiervan te delen met de mbo-instellingen. Alhoewel er geen reden is om te twijfelen aan de beschreven en genomen maatregelen, dient dit wel technisch te worden vastgesteld. Het reeds eerdergenoemde beveiligingsassessment had een beperkte scope in het kader van het aansluiten van CA op DigiD, maar geeft wel een beeld van de genomen beveiligingsmaatregelen. Het uitvoeren van een nieuwe audit op de gehele voorziening CA staat de live-gang niet in de weg. Hierbij wordt in overweging gegeven om deze audit of inspectie in samenhang uit te laten voeren met VVA, en de daaruit voortvloeiende aanbevelingen uit te (laten) voeren. Het uitvoeren van deze audit of inspectie wordt gezien als noodzakelijk, daarmee wordt het risico voor nadelige gevolgen voor de rechten en vrijheden van betrokken aspirant-studenten ingeschat op gemiddeld.

Een ander risico is misbruik van de persoonsgegevens van de aspirant-student. Andere leerlingen kunnen zich aanmelden, een aanmelding wijzigen of intrekken of contactgegevens wijzigen. Doordat het inloggen geschiedt met DigiD (later e-ID) wordt dit risico beperkt tot een minimum nu er gebruik wordt gemaakt door een door de overheid gebruikt identificatie- en authenticatiemiddel en 2FA. Voor studenten zonder PGN (of DigiD) is voorzien in een proces met vergelijkbare waarborgen: na melding van de aspirant-student dat hij interesse heeft in een opleiding, is de betreffende mbo-instelling verantwoordelijk voor de identificatie en authenticatie van de student. De risico's op dit vlak zijn beperkt zodat er geen verdere maatregelen nodig zijn.

De voorziening Centraal Aanmelden maakt gebruik van berichtuitwisseling met de SIS van iedere mbo-instelling. Dat betekent dat de veiligheid van de verwerkte en uitgewisselde persoonsgegevens van aspirant-studenten mede afhankelijk is van de beveiliging van iedere SIS. Het is niet mogelijk om in het kader van deze DPIA daar een oordeel over te geven. Met de SIS-leveranciers in het mbo zijn afspraken gemaakt over het implementeren van de maatregelen die het (veilig) koppelen op Centraal Aanmelden (en VVA) mogelijk maken. Iedere mbo-instelling heeft zelf afspraken met de SIS-leverancier en is verantwoordelijk voor het maken van afspraken met de eigen SIS-leverancier in het kader de verwerkersovereenkomst. Het niet of onvoldoende regelen van afspraken met de SIS-leveranciers kan nadelige gevolgen hebben voor de privacy van aspirant-studenten. Daar staat tegenover dat alle mbo-instellingen afspraken zullen hebben gemaakt in een verwerkersovereenkomst, temeer nu de SIS een belangrijk systeem voor mbo-instellingen is. Het risico voor de privacy van aspirant-studenten wordt daarom ingeschat op laag.

Risico's m.b.t. uitwisseling gegevens door/van/met CA en VVA

Er kunnen zich tal van gebeurtenissen voordoen waardoor het gegevensverkeer niet correct verloopt. In de risicoanalyse worden dergelijke gebeurtenissen geïnventariseerd, wordt de kans dat een gebeurtenis zich voordoet ingeschat en wordt ingeschat welke gevolgen zo'n gebeurtenis heeft voor de betrokkene.

We richten ons bij deze risicoanalyse op het proces tussen de voorziening CA en de mbo-instellingen.

Bij berichtenverkeer 'dat niet correct verloopt' maken we onderscheid tussen de volgende situaties:

1. Berichten worden ten onrechte niet of te laat verzonden: door het tijd-kritisch karakter van de aanmelding kunnen de gevolgen van te laat verzenden vergelijkbaar zijn met niet verzenden.
2. Berichten worden op het verkeerde adres bezorgd
3. Gegevens worden ten onrechte openbaar gemaakt.

Ad 1. Berichten worden ten onrechte niet of te laat verzonden

a. Programmatuur werkt niet goed

De kans dat de programmatuur op de koppelpunten niet goed werkt is relatief laag. Het betreft organisaties die digitale dienstverlening als kerntaak hebben en die het ontwerp als medeopstellers zeer goed kennen. Tevens is een SLA afgesproken tussen de Coöperatie MBO voorzieningen U.A. en Topicus.

b. Foutsituaties niet opgelost

De kans dat de programmatuur bij de partijen in de domeinen niet goed werkt is iets groter. De dienstverlening wordt geleverd door leveranciers van administratieve systemen. Binnen het CA-project is/wordt met de SIS-leveranciers gesproken en er is afstemming tussen betrokken partijen over de functionele eisen voor CA. Er is geen dwingende sturing op de leveranciers mogelijk, anders dan via afspraken (overeenkomsten) tussen onderwijsinstellingen en hun eigen SIS-leverancier.

In het PvE is de regel dat een partij die een foutsituatie veroorzaakt daar bericht van krijgt en dan gehouden is om die zelf op te lossen. Wanneer dat niet gebeurt, wordt een bericht ten onrechte niet verzonden. Scholen dienen zich bewust te zijn dat de formatie op de studentenadministraties voldoende is om het systeem te kunnen ondersteunen.

Ad 2. Berichten worden op het verkeerde adres bezorgd.

a. Aangeleverde of ingelezen gegevens student in SIS niet up to date

Dit risico wordt als zeer klein ingeschat aangezien de scholen afhankelijk zijn van de juiste informatie in hun SIS. Met CA voert de aspirant-student gegevens zelf in CA in. Het SIS is gekoppeld met externe systemen zoals RON (DUO) waar informatie wordt

aangeleverd. Het risico op verouderde gegevens ligt dan ook meer bij de mbo-instelling die de info in het SIS up to date moet houden. Voor contactgegevens zijn de risico's elders in dit hoofdstuk overwogen.

b. Programmatuur werkt niet goed

Ook dit risico wordt als klein ervaren. Het PvE noemt een aantal services die bedoeld zijn om tot juiste adressering van berichten te komen. Daar is juiste adressering van afhankelijk. Tevens is een SLA met Topicus overeenkomen om de juiste werking te kunnen blijven garanderen.

Ad 3. Gegevens worden onbedoeld openbaar gemaakt.

a. Autorisaties in administratieve systemen niet goed ingeregeld

Dit is een klein risico aangezien dit standaard geregeld moet zijn bij scholen en bij (sub)verwerker. Daar komt bij dat een student kiest voor het aanmelden, dit proces kan niet worden gestart door de mbo-instellingen. Er is sprake van een geautomatiseerde uitwisseling waar informatie 'binnen de systemen van de mbo-instellingen' wordt afgeleverd. Koppelingen worden centraal aangemaakt, informatie is afkomstig uit de Registratie Instellingen en Opleidingen (RIO). Van inloggen in CA door mbo-instellingen, is geen sprake. Studenten loggen in met hun DigiD (e-ID), welk toegangsproces aan strenge eigen van Logius moet voldoen. Met (sub)verwerker is de verplichting afgesproken de noodzakelijke geheimhoudingsovereenkomsten af te sluiten met personeel.

b. Onvoldoende beveiligingsniveau niet of verkeerd ingeschat, wat leidt tot datalekken.

Zeer klein risico aangezien de uitgewisselde berichten versleuteld zijn. Het beveiligingsniveau is gebaseerd op de BIV-classificatie van het Certificeringsschema.

c. Mogelijke inbreuk op persoonlijke levenssfeer betrokkene

Voor het aanmeldbericht vanuit mbo-instellingen richting een SIS, is het risico klein. Voor zover er al informatie over aspirant-studenten bij verkeerde mbo-instellingen als ontvanger wordt afgeleverd, geldt dat iedere ontvangende mbo-instelling medeverantwoordelijke is in het kader van de dienstverlening van CA. Mbo-instellingen zijn gehouden aan de (geheimhoudings)verplichtingen op grond van de AVG, WEB en afspraken in de verwerkersovereenkomst.

Voor zover koppelingen met DigiD (e-ID) niet werken, bijvoorbeeld als het PGN/BSN niet goed gematcht wordt waardoor BRON verkeerde gegevens aanlevert) speelt er een groter probleem dat alle gebruikers van DigiD zal treffen. Dit risico is ook benoemd bij DigiD die haar maatregelen richt op het voorkomen van dit risico. De kans dat zich dit voordoet is dan ook klein.

H. Conclusies en aanbevelingen

Op basis van het onderzoek dat we in het kader van deze DPIA hebben uitgevoerd, is de conclusie dat de verwerking van persoonsgegevens van (aspirant-)studenten in de voorziening Centraal Aanmelden een beperkt risico inhoudt voor de rechten en vrijheden van deze aspirant-studenten.

De geconstateerde risico's zijn te classificeren als laag tot gemiddeld. De door de Coöperatie genomen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen binnen Centraal Aanmelden om de bescherming van persoonsgegevens te garanderen, zijn gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is niet gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moet leiden tot een 'voorafgaande raadpleging' zoals omschreven in artikel 36 AVG.

In het kader van deze DPIA, komen we op een aantal aanbevelingen waardoor de risico's (nog meer) gemitigeerd worden. Gelet op artikel 35 lid 1 AVG is het advies dat de bij de voorziening CA aangesloten mbo-instellingen (als verwerkingsverantwoordelijken) samen met de Coöperatie MBO Voorzieningen (als verwerker), voorafgaand aan het gebruik van de voorziening Centraal Aanmelden, hebben overwogen welke maatregelen op welk tijdpad worden overgenomen en (aangepast) geïmplementeerd.

Het al dan niet gebruik (gaan) maken van de voorziening Centraal Aanmelden is en blijft de verantwoordelijkheid van ieder College van Bestuur van een mbo-instelling. Zeker omdat de werking van Centraal Aanmelden afhankelijk is van de SIS van de mbo-instelling, is het raadzaam dat iedere mbo-instelling voor de door haar gebruikte SIS beoordeelt of de genomen maatregelen een passend beschermingsniveau bieden.

De aanbevelingen die op basis van de DPIA worden gedaan, zijn:

1. Onduidelijkheid over rolverdeling in het kader van gezamenlijke verwerkingsverantwoordelijkheid mbo-instellingen:
 - a. maken van afspraken over de gezamenlijke verwerkingsverantwoordelijkheid
 - b. aanpassingen hierover in de verwerkersovereenkomsten
 - c. communicatie hierover met mbo-instellingen en informatievoorziening aan gebruikers van CA.
2. Documenteren van de bewaartermijnen (bij voorkeur in bewaarbeleid) voor bewaren studentgegevens binnen CA en de
 - a. termijn voor bewaren en vernietiging van deze gegevens (dit zou drie respectievelijk een jaar zijn)
 - b. mogelijkheden aspirant-student voor verlengen van de termijn voor bewaren van deze student-gegevens in CA
 - c. termijn voor classificeren, bewaren en vernietigen data over meervoudig aanmelden
 - d. communicatie over bewaartermijnen aan mbo-instellingen en aspirant-studenten.

3. Eenmalige uitwisseling aanmelding – integriteit (actualiteit) persoonsgegevens: communicatie aan mbo-instellingen over eenmalige uitwisseling en gevolgen hiervan voor integriteit van aangeleverde persoonsgegevens
4. Informatie aan mbo-instellingen over intrekken van aanmelding: gevolgen voor de informatie in de SIS. Om bovenmatige verwerking van persoonsgegevens te voorkomen verdient het aanbeveling mbo-instellingen te informeren over de gevolgen van het intrekken van de aanmelding en de gevolgen daarvan voor de ontvangen persoonsgegevens van de aspirant-student.
5. Bij gebruik en analyse van de data voor meervoudig aanmelden, bestaat de (theoretische) mogelijkheid dat gegevens onbedoeld herleidbaar zijn tot individuele aspirant-studenten. Er is hiervoor een maatregel geïmplementeerd dat informatie over groepen aspirant-studenten kleiner dan 5 niet getoond worden, maar deze informatie ontbreekt in de documentatie.
6. De DPIA is beperkt tot een beoordeling van de beschikbare documentatie. In het kader van artikel 26 lid 3 onder h AVG verdient het aanbeveling om op korte termijn (van circa 3 tot 5 maanden) een onafhankelijke audit of inspectie op CA uit te laten voeren. Omdat het gebruik van CA mede afhankelijk is van VVA, is het dringende advies om de audit of inspectie mede uit te (laten) voeren op VVA. Belangrijke vragen bij deze audit of inspectie zijn of de in de documentatie beschreven beveiligingsmaatregelen aangetroffen zijn binnen CA (en VVA), werkend zijn en daarmee een passend beschermingsniveau bieden. Deze scope is breder dan het reeds eerder uitgevoerde beveiligingsassessment in het kader van DigiD.
7. In de documentatie is weinig beschreven over communicatie aan aspirant-studenten en transparantie over het gebruik van hun persoonsgegevens. Het verdient aanbeveling dat de Coöperatie MBO Voorzieningen de aspirant-studenten (pro-)actief informeren in een voor hen begrijpelijke taalniveau over de omgang met hun privacy en de verwerking van persoonsgegevens.
8. Het gebruik van de voorziening CA is mede afhankelijk van de SIS van iedere mbo-instelling. Het verdient aanbeveling om mbo-instellingen hierop te wijzen en hun afspraken met hun SIS-leverancier – zo nodig - aan te passen op het gebruik van CA en VVA.