

25 juli 2024

Rapportagemodel DPIA Rijksdienst - OnTrac

MBO Raad

Versie 1.0

Voor MBO Raad

Door ICTRecht



Inhoudsopgave

1. Managementsamenvatting	3
2. Beschrijving kenmerken gegevensverwerking	6
2.1 Voorstel	6
2.2 Persoonsgegevens	7
2.3 Gegevensverwerkingen	9
2.4 Technieken en methoden van de gegevensverwerkingen	9
2.5 Verwerkingsdoeleinden	9
2.6 Betrokken partijen	10
2.7 Belangen bij de gegevensverwerkingen	12
2.8 Verwerkingslocaties	12
2.9 Juridisch en beleidsmatig kader	13
2.10 Bewaartermijnen	14
3. Beoordeling rechtmatigheid gegevensverwerkingen	16
3.1 Rechtsgrond	16
3.2 Bijzondere persoonsgegevens	17
3.3 Doelbinding	18
3.4 Noodzaak en evenredigheid	19
3.5 Rechten van betrokkenen	20
4. Beschrijving en beoordeling risico's voor betrokkenen	24
5. Maatregelen en restrisico's	26
6. Ondertekening	30

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., gevraagd om een centrale Data Protection Impact Assessment ('DPIA') uit te voeren ten aanzien van OnTrac.

OnTrac is een SaaS-oplossing die wordt geleverd door Leverancier Xebic Onderwijs B.V. ('Xebic'). OnTrac kan gebruikt worden door scholen in het middelbaar beroepsonderwijs ('mbo'). Mbo-instellingen ('de mbo-instellingen') kunnen door middel van OnTrac de totale examinering organiseren. OnTrac vermindert de logistieke- en administratieve druk op begeleiders en studentenadministratie. Bovendien kunnen onderwijsinstellingen de voortgang rond elk examen inzien en zo nodig bijsturen.

Er worden veel persoonsgegevens verwerkt door middel van OnTrac. Aangezien het gaat om een grootschalige verwerking van persoonsgegevens, 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. Hieronder volgen de geconstateerde risico's en voorgestelde maatregelen om deze risico's te mitigeren.

	Risico	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 binnen OnTrac. Daarbij dient onder andere uitgelegd te worden welke persoonsgegevens van studenten en medewerkers verstrekt worden aan Xebic, hoelang de gegevens bewaard blijven en welke beveiligingsmaatregelen zijn getroffen.	Kans	X	
			Schade		
			Na het treffen van maatregelen is het restrisico laag.		
2	Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen in OnTrac 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.	Kans	X	
			Schade		
			Na het treffen van maatregelen is het restrisico laag.		

3	Het risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk. De persoonsgegevens die door surveillanten kunnen worden ingezien, zijn niet allemaal noodzakelijk voor het uitoefenen van diens functie en het bereiken van de doeleinden van die verwerkingen. Indien meer persoonsgegevens worden verwerkt dan noodzakelijk, wordt niet voldaan aan het beginsel van dataminimalisatie, en is de verwerking, voor zover deze buitensporig is, onrechtmatig.	Idealiter dient in OnTrac te worden ingeregeld dat surveillanten niet meer gegevens kunnen inzien dat noodzakelijk is voor de surveillance die zij doen, bijvoorbeeld door autorisaties in te perken voor deze categorie personen.	Kans   Schade   Na het treffen van maatregelen is het restrisico laag.
4	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 in OnTrac. Dat leidt tot 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 maximale bewaartermijn zou bijvoorbeeld op 6 maanden na beëindiging van de laatste onderwijsinschrijving kunnen worden gesteld, al dienen individuele mbo-instellingen de gehanteerde termijn zelf te motiveren. Ter handhaving van de termijnen zou als optie geautomatiseerde verwijdering van gegevens kunnen worden ingebouwd als de ingestelde termijn is verstreken. De mbo-instelling is zelf verantwoordelijk voor de geautomatiseerde verwijdering. Wij adviseren de mbo-instellingen om de geautomatiseerde verwijdering van reeds vastgestelde termijnen in te voeren.	Kans   Schade   Na het treffen van maatregelen is het restrisico laag.
5	Het risico bestaat dat er geen passende afspraken zijn gemaakt met partijen	De mbo-instelling dient een verwerkersovereenkomst	Kans   Schade  

	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.	t te sluiten met haar verwerkers. Naast Xebic, waarvoor er al een verwerkersovereenkomst ligt, dient met de leveranciers van bronssystemen een verwerkersovereenkomst te worden gesloten.	Na het treffen van maatregelen is het restrisico laag.
6	Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op 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 in OnTrac te informeren over de verwerking van hun persoonsgegevens. Dit dient zij te doen door een privacyverklaring voor studenten en een interne privacyverklaring voor medewerkers beschikbaar te stellen bij de inlogpagina van OnTrac. De privacyverklaring is daarmee vindbaar op zowel de website van de mbo-instelling als bij het inlogscherms van OnTrac.	Kans X Schade Na het treffen van maatregelen is het restrisico laag.

2. 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.

2.1 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., gevraagd om een centrale Data Protection Impact Assessment ('DPIA') uit te voeren ten aanzien van OnTrac.

OnTrac is een SaaS-oplossing die wordt geleverd door Leverancier Xebic Onderwijs B.V. ('Xebic'). OnTrac kan gebruikt worden door scholen in het middelbaar beroepsonderwijs ('mbo'). Mbo-instellingen ('de mbo-instellingen') kunnen door middel van OnTrac de totale examinering organiseren. OnTrac vermindert de logistieke- en administratieve druk op begeleiders en studentenadministratie. Bovendien kunnen onderwijsinstellingen de voortgang rond elk examen inzien en zo nodig bijsturen.

OnTrac kent verschillende rollen, en per rol verschillende rechten. Hiermee blijft het gebruik van OnTrac eenvoudig omdat iedere gebruiker een "gepersonaliseerde view" krijgt. OnTrac toont namelijk alleen die informatie en schermen die een gebruiker nodig heeft voor zijn functie of rol. OnTrac maakt het daarnaast mogelijk dat medewerkers en studenten met hun eigen instellingsaccount kunnen inloggen op OnTrac. Hierdoor hoeven scholen geen aparte gebruikersaccounts meer aan te maken, maar kunnen bestaande accountgegevens (her)gebruikt worden. Voor medewerkers dient nog steeds het account, met daaraan de juiste rollen en rechten gekoppeld, te worden aangemaakt. Bovendien kunnen op het schoolnetwerk ingelogde gebruikers direct verder werken met OnTrac via het zogeheten 'single sign-on' principe.

OnTrac is een webapplicatie en wordt als online dienst beschikbaar gesteld. OnTrac heeft een service-georiënteerde architectuur (Triple A) specifiek ontworpen om eenvoudig te kunnen koppelen met softwaresystemen zoals Osiris, Facet, Remindo, TOA, Magister, Eduarte, Education online en PeopleSoft.

Er worden veel persoonsgegevens verwerkt door middel van OnTrac. Aangezien het gaat om een grootschalige verwerking van persoonsgegevens, 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.

In deze DPIA worden de verwerkingen van persoonsgegevens in het kader van OnTrac getoetst aan de Algemene verordening gegevensbescherming¹ ('AVG') en de Uitvoeringswet AVG² ('UAVG'). Aanvullend is rekening gehouden met de richtlijn van het Europees Comité voor gegevensbescherming (voorheen: Artikel 29-Werkgroep) inzake het uitvoeren van een DPIA.³

Als input zijn er verschillende documenten geraadpleegd en hebben er verschillende overleggen plaatsgevonden tussen stakeholders, waaronder leverancier Xebic en ICTRecht.

Aangezien dit een centrale DPIA betreft wordt er enkel ingegaan op risico's en aandachtspunten met betrekking tot het algemene gebruik van OnTrac. In de tekst wordt waar nodig aangegeven waar specifieke aandachtspunten voor mbo-instellingen zijn zodat zij dit zelf of gezamenlijk met Xebic kunnen adresseren. Daarnaast is er ook een whitepaper beschikbaar die is opgesteld aan de hand van deze DPIA. In deze whitepaper zijn de acties die de mbo-instellingen moeten nemen ook opgenomen.

2.2 Persoonsgegevens

Deze paragraaf beschrijft alle persoonsgegevens die worden verwerkt, alsmede hoe deze persoonsgegevens worden gekwalificeerd en wat de bron is van deze gegevens.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegevens	Bron
Studenten	Contactgegevens	Voornaam	Gewoon en bijzonder	Student-informatiesysteem ('SIS')
	Studentennummer	Voorletters		
	Medische gegevens (wel/geen hulpmiddelen)	Achternaam		
	Examenresultaten	Geslacht		
	Traject voortgang registratie	Geboortedatum		
	Studentenbegeleiding rapportage	E-mailadres		
	Aanwezigheidsregistratie	Wachtwoord		
		Telefoonnummer		
		Hulpmiddelen (gezondheidsgegevens)		

¹ 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).

² 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).

³ 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.

Medewerkers ⁴	Contactgegevens Personeelsnummer	Straatnaam (optioneel)	Gewoon	Mede- werkers mbo- instelling
		Huisnummer (optioneel)		
		Huisnummer toevoeging (optioneel)		
		Postcode (optioneel)		
		Woonplaats (optioneel)		
		Naam studierichting		
		Verwachte einddatum opleiding		
		Vooropleiding		
		Gebruikersnaam		
		Medewerkerscode		
		Voornaam		
		Tussenvoegsel		
		Achternaam		
		E-mailadres		
		Organisatie		
		Rol		

Bovenstaande biedt een overzicht van de persoonsgegevens die mogelijk verwerkt worden door middel van OnTrac. Dit betreft echter een indicatie gebaseerd op de mogelijkheden die OnTrac biedt. 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 door middel van OnTrac, is afhankelijk van de informatie die medewerkers van de mbo-instelling opnemen in OnTrac.

De persoonsgegevens kunnen op meerdere manieren in OnTrac terechtkomen. Wanneer er een gekoppelde applicatie is dat als bron kan dienen voor een persoonsgegeven, zoals een studentinformatiesysteem, is het mogelijk om vanuit het studentinformatiesysteem persoonsgegevens te sturen naar OnTrac. Een andere optie is dat studenten, medewerkers of contactpersonen zelf informatie toevoegen aan OnTrac.

⁴ Onder 'medewerkers' worden alle personen geschaard die onder het gezag van de mbo-instelling persoonsgegevens verwerken in de breedste zin van het woord, waaronder werknemers en extern ingehuurd personeel.

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 OnTrac. OnTrac biedt een oplossing voor het organiseren van de totale examinering. Wel blijft de mbo-instelling de verantwoordelijke voor de verwerking en heeft uiteindelijk zeggenschap over welke persoonsgegevens er wel/niet verwerkt worden via OnTrac.

2.3 Gegevensverwerkingen

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

Gegevensverwerking	Categorieën persoonsgegevens
De verwerking van persoonsgegevens van de student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Gewoon en bijzonder

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 OnTrac.

De gegevensverwerking die hier centraal staat is de verwerking van gewone en bijzondere persoonsgegevens van de student en de medewerker ten behoeve van de administratie rondom het examineringsproces.

De persoonsgegevens kunnen op meerdere manieren in OnTrac terechtkomen. Wanneer er een gekoppelde applicatie is dat als bron kan dienen voor een persoonsgegeven, zoals een studentinformatiesysteem, is het mogelijk om vanuit het studenteninformatiesysteem persoonsgegevens te sturen naar OnTrac. Een andere optie is dat medewerkers zelf informatie toevoegen aan OnTrac.

2.4 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.

OnTrac is een cloud/SaaS-oplossing. 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.⁵ Dit brengt echter ook risico's met zich mee. Het is daarom belangrijk om contractuele afspraken te maken met de leverancier over de verwerking van persoonsgegevens. Onder de koppen 'Risico's voor betrokkenen' en 'Maatregelen' wordt hier verder op ingegaan.

2.5 Verwerkingsdoeleinden

Deze paragraaf beschrijft de doeleinden van de verwerkingen.

⁵ Uitleg bij het Rijksmodel, p. 46.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
De verwerking van persoonsgegevens van de student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Het administreren van het examineringsproces. [Aanvullende, nadere verwerkingsdoeleinden te bepalen door mbo-instelling, bijvoorbeeld: • het regelen van inschrijvingen voor examens • het afnemen van een examen • het registreren en afhandelen van incidenten • het surveilleren bij examens]	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan OnTrac 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 paragraaf 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. Xebic is, als leverancier van de SaaS-oplossing OnTrac, aan te merken als de verwerker 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. De mbo-instelling bepaalt het doel en de middelen van de gegevensverwerking, en het is aan Xebic om slechts in opdracht van de mbo-instelling persoonsgegevens te verwerken.

Persoonsgegevens mogen enkel worden gebruikt voor het doel waarvoor ze zijn verzameld, of voor doeleinden die daarmee verenigbaar zijn.⁶ 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. De administratie omtrent de examinering is hier onderdeel van. Het is niet toegestaan om deze gegevens voor andere, onverenigbare doeleinden, te gebruiken.

Voor het gebruik van OnTrac 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 het administreren van het examineringsproces. De middelen van de verwerking zien op de manier waarop de verwerking praktisch vorm krijgt, in dit geval OnTrac.

2.6 Betrokken partijen

Deze paragraaf beschrijft alle partijen die betrokken zijn, alsmede welke rol deze vervullen, onderverdeeld in: verwerkingsverantwoordelijke, gezamenlijke

⁶ Artikel 5 (1) (b) Algemene verordening gegevensbescherming.

verwerkingsverantwoordelijke, verwerker, subverwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend is tevens benoemd welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens.

Naam partij	Rol partij	Functies/afdelingen	Persoonsgegevens
Mbo-instelling	Verwerkingsverantwoordelijke	n.v.t.	Gewoon en bijzonder
Xebic	Verwerker	Supportmedewerkers, TAB-Team en Hosting & Beheer	Gewoon en bijzonder
Microsoft Azure	Subverwerker	n.v.t.	Gewoon en bijzonder
Studenten	Betrokkene	n.v.t.	Gewoon en bijzonder
Medewerkers	Betrokkene	n.v.t.	Gewoon
Solcon N.V.	Derde	n.v.t.	n.v.t.
SIS (Caci, Educus, Schoolmaster, Fringe, UOCGMarket, [...])	Verwerker	n.v.t.	Gewoon en bijzonder
Federatief inloggen (SurfConext, Kennisnet Entree, [...])	Verwerker	n.v.t.	Gewoon en bijzonder
DUO (Facet)	Derde	n.v.t.	Gewoon en bijzonder
Bureau ICE (TOA)	Verwerker	n.v.t.	Gewoon en bijzonder

Diverse partijen zijn betrokken bij de verwerking van persoonsgegevens door middel van OnTrac. 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 middel van OnTrac aan te merken als verwerkingsverantwoordelijke. De mbo-instelling bepaalt immers het doel en de middelen van de gegevensverwerking in het kader van OnTrac. Xebic wordt ingeschakeld door de mbo-instelling om de gegevensverwerking te verrichten. Xebic verwerkt dus in opdracht van de mbo-instelling de persoonsgegevens en is dus aan te merken als verwerker in de zin van de AVG.

Zoals blijkt uit de verwerkersovereenkomsten die worden gehanteerd, schakelt Xebic op haar beurt één subverwerker in: Microsoft Azure.

Daarnaast biedt OnTrac de mogelijkheid tot het koppelen met diensten van derde partijen, die al dan niet verwerker kunnen zijn van de mbo-instelling. In opdracht van de verwerkingsverantwoordelijke kan Xebic persoonsgegevens doorgeven aan derde partijen waarmee OnTrac een koppeling heeft. Ook wordt Solcon N.V. ingeschakeld ten behoeve van de hosting. De medewerkers van Solcon N.V. hebben geen toegang tot de persoonsgegevens. Solcon N.V. is housing-leverancier: de onderliggende hardware is eigendom van Xebic en valt daarmee onder de verantwoordelijkheid van Xebic. Deze partij dient daarom te worden gekwalificeerd als derde.

Tot slot dienen de studenten en medewerkers te worden aangemerkt als betrokkenen in de zin van de AVG.

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

2.7 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 Xebic	- Voorzien in onderwijs - Bedrijfsbelangen - Financiële en commerciële belangen - Voldoen aan de overeenkomst met de mbo-instelling
Studenten Medewerkers	- Volgen van onderwijs aan mbo-instelling - Uitvoeren van werkzaamheden voor mbo-instelling in het kader van de arbeidsovereenkomst

De mbo-instelling heeft slechts één belang, het voorzien in onderwijs.

Xebic heeft een bedrijfsbelang, financieel en/of commercieel belang en daarnaast dient zij te voldoen aan de overeenkomst met de mbo-instelling.

De studenten hebben slechts één belang, het volgen van onderwijs aan de mbo-instelling. De medewerkers hebben er belang bij om hun werkzaamheden uit te voeren voor de mbo-instelling in het kader van de arbeidsovereenkomst.

2.8 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 student en	Opslag en verwerking persoonsgegevens:	n.v.t.	n.v.t.

medewerker ten behoeve van de administratie rondom het examineringsproces.	• Apeldoorn (Solcon N.V.) – Hosting platform ten behoeve van de applicaties • Dronten (Solcon N.V.) – Externe opslag back-ups productieplatform • Amsterdam (Microsoft Azure), Opslag Documenten en hosting Integratieplatform		
--	--	--	--

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.

Xebic is een in Nederland gevestigde organisatie. Zij maakt gebruik van één subverwerker: Microsoft. Microsoft 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 afsluiten van Standard Contractual Clauses (SCC's) niet meer nodig is en er geen aanvullende maatregelen worden getroffen hoeven te worden. Het is wel vereist dat Microsoft aangesloten is bij het Data Privacy Framework. Op het moment van schrijven is Microsoft aangesloten.

2.9 Juridisch en beleidsmatig kader

Deze paragraaf beschrijft alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn⁷ zijn niet genoemd.

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
De verwerking van persoonsgegevens van de student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Wet educatie en beroepsonderwijs, Model documentair structuurplan	Artikel 7.4.8 lid 1, 2 en 5, artikel 8.1.1 en artikel 8.1.1a WEB

Wet educatie en beroepsonderwijs

⁷ 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.

De Wet educatie en beroepsonderwijs ('WEB') regelt verschillende vormen van beroepsonderwijs en volwasseneneducatie, waaronder het middelbaar beroepsonderwijs. Van belang voor verwerkingen binnen de applicatie 'OnTrac' is dat de WEB bepalingen bevat omtrent het regelen van examinering, het informeren van studenten daarover en de inschrijving van studenten voor examenvoorzieningen. Zo ligt de algemene taak om zorg te dragen voor een goede organisatie en kwaliteit van het onderwijsprogramma en examinering bij het bevoegd gezag, en dienen personen die gebruik willen maken van een examenvoorziening zich daartoe in te schrijven als student. OnTrac biedt faciliteiten om inschrijvingen te regelen en in te zien, om incidenten te administreren en besluiten daarover weer te geven en om de afname van examens soepeler te laten verlopen.

Ten aanzien van de verwerkingen die plaatsvinden in het kader van administratie rondom het examineringsproces, zijn de mbo-instellingen die gebruik maken van OnTrac zelf verwerkingsverantwoordelijke.

Model documentair structuurplan

Op mbo-instellingen, als zijnde verwerkingsverantwoordelijke, rust de plicht uit de AVG tot opslagbeperking van persoonsgegevens. Dat betekent dat zij bewaartermijnen moeten vaststellen voor de persoonsgegevens die zij verwerken. Door de MBO Raad is hiertoe als handreiking een model documentair structuurplan opgesteld, dat individuele mbo-instellingen kunnen gebruiken bij het vaststellen van hun bewaartermijnen.

2.10 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.

Gegevens-verwerking	Verwerking doeleinde	Categorie Persoons-gegevens	Bewaar-termijn	Motivatatie bewaar-termijn
De verwerking van persoonsgegevens van de student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Het administreren van het examinering proces. [Aanvullende verwerkings doeleinden te bepalen door mbo-instelling, bijvoorbeeld:] • het regelen van inschrijvingen voor examens	Contactgegevens Studenten-/personeelsnummer Medische gegevens (wel/geen hulpmiddelen) Examenresultaten Traject voortgang registratie Studentenbegeleiding rapportage	[in te vullen door de mbo-instelling] Maximaal 6 maanden na beëindiging van de laatste onderwijsinschrijving.	[in te vullen door de mbo-instelling]

	• het afnemen van een examen • het registreren en afhandelen van incidenten • het surveilleren bij examens	Aanwezigheidsregistratie		
--	--	--------------------------	--	--

Invoer en handhaving bewaartermijnen

Mbo-instellingen dienen zelf door het invullen van invulvelden bewaartermijnen in te voeren in OnTrac; deze worden niet door leverancier Xebic vastgesteld of ingevuld. Na verloop van de ingevoerde bewaartermijn, worden de betreffende gegevens gemarkeerd voor verwijdering, waarna de mbo-instelling de gegevens zelf dient te verwijderen. Bewaartermijnen worden in OnTrac dus niet geautomatiseerd gehandhaafd.

Toelichting bewaartermijnen

Zoals gezegd is OnTrac een integratiesysteem, waarbij veelal persoonsgegevens uit andere systemen worden ingeladen. Dat 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 OnTrac en persoonsgegevens die worden opgeslagen in de bronsystemen zoals het SIS. Indien persoonsgegevens al buiten OnTrac worden bewaard, is het niet altijd noodzakelijk alle persoonsgegevens in OnTrac even lang te bewaren.

Bij beëindiging van de laatste onderwijsinschrijving wordt OnTrac inactief ten aanzien van de betreffende student. Individuele mbo-instellingen dienen in te stellen na hoeveel maanden de betreffende student vervolgens uit OnTrac wordt verwijderd. Voordat verwijdering heeft plaatsgevonden kan het account van de betreffende student worden geheractiveerd. Na verwijdering dient een nieuwe aanmelding van student te worden gedaan.

De uiterste bewaartermijn die mbo-instellingen voor persoonsgegevens in OnTrac dienen vast te stellen, is dus gekoppeld aan de beëindiging van de laatste onderwijsinschrijving van een bepaalde student. Die zou bijvoorbeeld gesteld kunnen worden op 6 maanden na beëindiging van de laatste onderwijsinschrijving. Op die wijze kan nog enige tijd rekening gehouden worden met een eventuele heractivering van het account. Mbo-instellingen dienen echter zelf te onderzoeken hoe lang zij de persoonsgegevens in OnTrac willen bewaren. Deze termijn dient dan te worden vastgesteld en door de instelling zelf te worden gemotiveerd. Voor verschillende verwerkingen of persoonsgegevens dienen uiteraard kortere bewaartermijnen gehanteerd te worden indien die verwerkingen niet meer strikt noodzakelijk zijn voor de gestelde doeleinden. Bij niet-naleving van de gestelde bewaartermijnen worden meer persoonsgegevens verwerkt dan noodzakelijk, en wordt dus de AVG overtreden.

3. Beoordeling rechtmatigheid gegevensverwerkingen

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

3.1 Rechtsgrond

Iedere gegevensverwerking moet op een wettelijke grondslag uit de AVG worden gebaseerd met bijbehorende voorwaarden. Persoonsgegevens mogen dus alleen in OnTrac worden gezet als hiervoor een wettelijke grondslag bestaat. Voor de verwerkingen van persoonsgegevens in OnTrac is de grondslag 'uitvoering van de overeenkomst' van groot belang. Hierbij moet sprake zijn van uitvoering van de overeenkomst met betrokkene, waarvoor de verwerking van diens persoonsgegevens noodzakelijk is.

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
De verwerking van persoonsgegevens van de student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Uitvoering van de overeenkomst	De verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan OnTrac gekoppelde systemen, is verenigbaar met het oorspronkelijke doeleinde van die verwerking, zoals toegelicht onder paragraaf 13. Voor deze verwerking hoeft dus geen nieuwe grondslag te worden gezocht. In het geval deze verenigbaarheid mocht ontbreken, zouden de verwerkingen, evenals de nieuwe verwerkingen, hun grondslag vinden in de uitvoering van de overeenkomst. Het verwerken van persoonsgegevens van studenten is noodzakelijk voor het uitvoeren van de inschrijving voor het onderwijs bij de betreffende onderwijsinstelling. Het bieden van de mogelijkheid tot het behalen van een examen is onderdeel van die inschrijving. Met gebruik van de faciliteiten van OnTrac moet de goede organisatie en kwaliteit van de

		examinering worden gewaarborgd. Het verwerken van persoonsgegevens van medewerkers is eveneens noodzakelijk voor de uitvoering van een overeenkomst, maar dan de (arbeids)overeenkomst met de betrokken medewerker. Door gebruik van OnTrac kunnen medewerkers hun werkzaamheden uitoefenen en studenten begeleiden.
--	--	--

Ten aanzien van de grondslag geldt dat, alhoewel er wettelijke bepalingen zijn opgenomen in de WEB omtrent de administratie rondom het examenproces (artikelen 7.4.8, 8.1.1 en 8.1.1a WEB), deze geen grondslag vormen voor de genoemde gegevensverwerkingen in OnTrac. De bepalingen vormen geen uitdrukking van taken van openbaar gezag, evenmin vormen zij een voldoende gespecificeerde wettelijke verplichting voor mbo-instellingen. Toestemming is in dit geval een zeer wankel basis, nu tussen mbo-instellingen en medewerkers een afhankelijkheidsrelatie bestaat, en verdedigbaar ook tussen de instelling en de student. Daarnaast kan de organisatie van examinering in gedrang komen als enkele studenten geheel of gedeeltelijk geen toestemming geven. Een gerechtvaardigd belang of de behartiging van vitale belangen is niet aan de orde.

De enige grondslag die de beoogde verwerkingen kan dragen, is die van de uitvoering van de overeenkomst. Ten aanzien van studenten zijn de verwerkingen noodzakelijk om uitvoering te geven aan de inschrijving bij de betreffende mbo-instelling, nu de mogelijkheid tot het behalen van een diploma in het kader van die inschrijving moet worden geboden. Georganiseerde examinering is daar onlosmakelijk aan verbonden. De verwerking van persoonsgegevens van medewerkers is noodzakelijk voor de uitvoering van de (arbeids)overeenkomst met deze medewerkers. Door gebruik van OnTrac kunnen medewerkers hun werkzaamheden uitvoeren, gedeeltelijk bestaande uit de begeleiding van studenten.

3.2 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.

Gegevensverwerking	Type bijzonder persoonsgegeven	Uitzonderingsgrond
De verwerking van persoonsgegevens van de student ten behoeve van de administratie rondom het examineringsproces.	Gegevens over gezondheid	Artikel 9 lid 2 sub g AVG jo. artikel 30 lid 2 sub a UAVG

De gegevens over gezondheid zien in dit geval op de hulpmiddelen die leerlingen ter beschikking hebben bij bepaalde examens. Voor studenten met dyscalculie wordt bijvoorbeeld bij rekenexamens weergegeven dat de betreffende student recht heeft op tijdsverlenging. In SIS staat geregistreerd dat de student in kwestie dyscalculie heeft, en op het moment dat deze wordt ingeschreven voor een rekenexamen komt het middel waarop hij recht heeft in het dashboard te staan. Uit het weergegeven hulpmiddel kan informatie over de mentale of fysieke gezondheid van de student worden afgeleid. Dit kwalificeert als een bijzonder persoonsgegeven, zodat een uitzonderingsgrond voor de verwerking van deze gegevens aanwezig moet zijn.

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

3.3 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 student en medewerker ten behoeve van de administratie rondom het examineringsproces.	Contactgegevens Studenten-/personeelsnummer Medische gegevens (wel/geen hulpmiddelen) Examenresultaten Traject voortgang registratie Studentenbegeleiding rapportage Aanwezigheidsregistratie	Het administreren van het examineringsproces. [Aanvullende verwerkingsdoeleinden te bepalen door mbo-instelling, bijvoorbeeld:] • het regelen van inschrijvingen voor examens • het afnemen van een examen • het registreren en afhandelen van incidenten • het surveilleren bij examens	Voor de verwerking van persoonsgegevens die al eerder werden verwerkt binnen de aan OnTrac 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.

Zoals eerder is aangegeven, is OnTrac een integratiesysteem waarbij reeds voorhanden persoonsgegevens uit gekoppelde applicaties kunnen worden ingeladen. Omdat de persoonsgegevens al verwerkt werden door mbo-instellingen, doet zich de vraag voor of de verwerking van persoonsgegevens ten behoeve van de administratie 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

worden 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 (administratie rondom het examineringsproces) is onlosmakelijk deel van het kunnen realiseren van de oorspronkelijke doeleinden. Aangezien hoofdzakelijk 'gewone' persoonsgegevens worden verwerkt, en wat betreft bijzondere persoonsgegevens enkel het beschikbare hulpmiddel (en niet de achterliggende medische reden) wordt verwerkt in OnTrac, leidt de aard van de gegevens niet tot een andere conclusie. Tot slot zijn de gevolgen voor betrokkenen gering, en heeft Xebic passende beveiligingsmaatregelen getroffen. De verdere verwerking van deze persoonsgegevens is dus verenigbaar.

Ten aanzien van medewerkers 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 inschrijving van een student voor een examen, een incident tijdens een examen of aanwezigheid bij een examen, speelt verenigbaarheid van de verwerking geen rol. Voor deze verwerkingen wordt teruggevallen op de grondslag 'uitvoering van de overeenkomst', zoals toegelicht onder paragraaf 11.

3.4 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 wordt één overkoepelende gegevensverwerking onderscheiden: de verwerking van student- en medewerkersgegevens ten behoeve van de administratie rondom het examineringsproces. Deze gegevensverwerking vindt plaats ten behoeve van één verwerkingsdoeleinde(n). In deze paragraaf zal ten aanzien van dit verwerkingsdoeleinde worden beoordeeld of de verwerking noodzakelijk en evenredig is voor het verwezenlijken van dit doeleinde. Indien de mbo-instelling aanvullende verwerkingsdoeleinden bepaalt, dient zij steeds te beoordelen of er sprake is van noodzakelijkheid en evenredigheid.

Proportionaliteit

Ten aanzien van de administratie rondom het examineringsproces is het noodzakelijk dat alle in paragraaf 2 genoemde persoonsgegevens worden gebruikt.

Subsidiariteit

Ten aanzien van de administratie rondom het examineringsproces is het noodzakelijk dat alle in paragraaf 2 genoemde persoonsgegevens worden gebruikt.

De verwerking van persoonsgegevens is derhalve noodzakelijk en evenredig. In afwijking van het voorgaande geldt voor de **surveillance door surveillanten** echter een andere afweging.

Proportionaliteit

Ten aanzien van de surveillance door surveillanten is het noodzakelijk dat zij kunnen inzien bij welke examens zij dienen te surveilleren, welke studenten daarbij aanwezig dienen te zijn en op welke hulpmiddelen zij recht hebben. In OnTrac kunnen surveillanten echter nog aanvullende informatie inzien per student, waaronder nog te volgen toetsen en behaalde resultaten. Voor het surveilleren is het niet noodzakelijk voor de surveillant om deze aanvullende informatie in te kunnen zien. Dat betekent dat voor dit onderdeel van de verwerking nog niet wordt voldaan aan het proportionaliteitsbeginsel. Het aantal verschillende persoonsgegevens dat kan worden ingezien, dient te worden gelimiteerd.

Subsidiariteit

Ten aanzien van de surveillance door surveillanten is het noodzakelijk dat zij kunnen inzien bij welke examens zij dienen te surveilleren, welke studenten daarbij aanwezig dienen te zijn en op welke hulpmiddelen zij recht hebben. Zonder inzicht te geven in deze informatie kan geen toezicht op de examinering worden georganiseerd.

3.5 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	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Studenten kunnen een deel van de verwerkte gegevens inzien op hun eigen student scherm en in hun eigen dashboard. Met enkel het student scherm wordt geen inzicht geboden in alle	n.v.t.

	verwerkingen in OnTrac, voor welke doeleinden dit gebeurt, op welke grondslag, etc. Dat betekent dat door middel van het student scherm niet wordt voldaan aan het recht van inzage. Indien door de betrokkene een verzoek tot recht van inzage wordt ingediend bij zowel Xebic als de mbo-instelling, volstaat enkel het student scherm niet om te voldoen aan dit recht. De betrokkene dient een overzicht te ontvangen van alle in art. 15 lid 1 AVG genoemde informatie.	
Recht op rectificatie en aanvulling	Indien door de betrokkene wordt geconstateerd dat onjuiste persoonsgegevens in OnTrac staan, kan een verzoek worden ingediend bij zowel Xebic als de mbo-instelling, zodat deze kunnen worden aangepast. [mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]	n.v.t.
Recht op vergetelheid	Indien een betrokkene gebruik wenst te maken van het recht op vergetelheid, dan kan een verzoek worden ingediend bij zowel Xebic als de mbo-instelling, zodat de persoonsgegevens kunnen worden gewist. [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 beperking van de	n.v.t.

verwerking, dan kan een verzoek worden ingediend bij zowel Xebic als de mbo-instelling, zodat de verwerking beperkt kan worden.

[mbo-instelling dient een procedure vast te stellen voor zowel medewerkers als studenten]

Recht op dataportabiliteit	Indien een betrokkene gebruik wenst te maken van het recht op dataportabiliteit, dan kan een verzoek worden ingediend bij zowel Xebic als de mbo-instelling, zodat de persoonsgegevens gedeeld kunnen worden. [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 e jo. art. 6 lid 1 f AVG. Daar is in dit geval geen sprake van.	n.v.t.
Recht op duidelijke informatie	Individuele instellingen hebben niet de mogelijkheid om hun privacyverklaring in te voeren in het systeem, aldus Xebic. Het informeren van studenten dient dan op een ander moment of andere locatie plaats te vinden, bijvoorbeeld op de eigen website.	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 als een verwerkingsverantwoordelijke 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 extra 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 (Xebic). Mocht een verzoek bij Xebic worden ingediend dan is het aan Xebic om het verzoek door te sturen naar 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.

Ten aanzien van de uitoefening van hun rechten door betrokkenen hebben wij betreffende het recht op duidelijke informatie en het recht van inzage een mogelijk probleem in compliance kunnen signaleren. Het is namelijk voor individuele mbo-instellingen niet mogelijk om bij in OnTrac te verwijzen naar hun privacy- en cookieverklaring, zodat via andere kanalen als de eigen website transparantie geboden moet worden over de verwerking van persoonsgegevens via OnTrac. Voor de beste vindbaarheid van relevante informatie voor betrokkenen zou een mogelijkheid kunnen worden ingebouwd om in OnTrac een link te plaatsen naar de privacy- en cookieverklaring van de betreffende mbo-instelling.

Ten aanzien van het (uitoefenen van het) recht van inzage is ook een probleem geconstateerd. Studenten kunnen een deel van de verwerkte gegevens inzien op hun eigen student scherm en in hun eigen dashboard. Met enkel het student scherm wordt geen inzicht geboden in alle verwerkingen in OnTrac, voor welke doeleinden dit gebeurt, op welke grondslag, etc. Dat betekent dat door middel van het student scherm niet wordt voldaan aan het recht van inzage.

Indien door de betrokkene een verzoek tot recht van inzage wordt ingediend bij zowel Xebic als de mbo-instelling, volstaat enkel het student scherm niet om te voldoen aan dit recht. De betrokkene dient een overzicht te ontvangen van alle in art. 15 lid 1 AVG genoemde informatie, wat een mbo-instelling dus mogelijk dient te maken middels een procedure buiten OnTrac.

4. Beschrijving en beoordeling risico's voor betrokkenen

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

In onderstaande tabel zijn verschillende risico's beschreven in het kader van de verwerking van persoonsgegevens door middel van OnTrac. 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

*De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.

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

Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen in OnTrac 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

Het risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk. De persoonsgegevens die door surveillanten kunnen worden ingezien, zijn niet allemaal noodzakelijk voor het uitoefenen van diens functie en het bereiken van de doeleinden van die verwerkingen. Indien meer persoonsgegevens worden verwerkt dan noodzakelijk, wordt niet voldaan aan het beginsel van dataminimalisatie, en is de verwerking, voor zover deze buitensporig is, onrechtmatig.

Laag

Midden

Laag

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 in OnTrac. Dat leidt tot 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

Laag

Hoog

Laag

(datalekken), verlies van vertrouwelijkheid, en dat betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen.

Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op 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

5. 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 middel van OnTrac. 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 werken met alle verwerkingen binnen OnTrac. Daarbij dient onder andere uitgelegd te worden welke persoonsgegevens van studenten en medewerkers verstrekt worden aan Xebic, hoelang de gegevens bewaard blijven en welke beveiligingsmaatregelen zijn getroffen.	Laag	mbo-instelling
Het risico bestaat dat de verwerkingsdoeleinden van verwerkingen in OnTrac 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
Het risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk. De persoonsgegevens die door surveillanten kunnen worden ingezien, zijn niet allemaal noodzakelijk voor het uitoefenen van diens functie en het bereiken van de doeleinden van die	Idealer dient in OnTrac te worden ingeregeld dat surveillanten niet meer gegevens kunnen inzien dat noodzakelijk is voor de surveillance die zij doen, bijvoorbeeld door autorisaties in te perken voor deze categorie personen.	Laag	mbo-instelling en Xebic

verwerkingen. Indien meer persoonsgegevens worden verwerkt dan noodzakelijk, wordt niet voldaan aan het beginsel van dataminimalisatie, en is de verwerking, voor zover deze buitensporig is, onrechtmatig.			
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 in OnTrac. Dat leidt tot 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 maximale bewaartermijn zou bijvoorbeeld op 6 maanden na beëindiging van de laatste onderwijsinschrijving kunnen worden gesteld, al dienen individuele mbo-instellingen de gehanteerde termijn zelf te motiveren. Ter handhaving van de termijnen zou als optie geautomatiseerde verwijdering van gegevens kunnen worden ingebouwd als de ingestelde termijn is verstreken. De mbo-instelling is zelf verantwoordelijk voor de geautomatiseerde verwijdering. Wij adviseren de mbo-instellingen om de geautomatiseerde verwijdering van reeds vastgestelde termijnen in te voeren.	Laag	mbo-instelling en Xebic
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	De mbo-instelling dient een verwerkersovereenkomst te sluiten met haar verwerkers. Naast Xebic, waarvoor er al een verwerkersovereenkomst ligt, dient met de leveranciers van bronsystemen een verwerkersovereenkomst te worden gesloten.	Laag	mbo-instelling

(datalekken), verlies van vertrouwelijkheid, en dat betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen.			
Het risico bestaat dat onvoldoende transparantie richting betrokkenen wordt geboden, zodat niet wordt voldaan aan de informatieplicht die op 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 in OnTrac te informeren over de verwerking van hun persoonsgegevens. Dit dient zij te doen door een privacyverklaring voor studenten en een interne privacyverklaring voor medewerkers beschikbaar te stellen bij de inlogpagina van OnTrac. De privacyverklaring is daarmee vindbaar op zowel de website van de mbo-instelling als bij het inlogscherf van OnTrac.	Laag	mbo-instelling en Xebic

6. 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)	[naam verantwoordelijke(n)]
Directie/afdeling verantwoordelijke(n)	[directie/afdeling verantwoordelijke(n)]
Functie verantwoordelijke(n)	[functie verantwoordelijke(n)]
Datum ondertekening	[datum ondertekening]
Handtekening	[handtekening]