Driving innovation together

DPIA Osiris

Systeem DPIA

Author(s)): Arnold Roosendaal, Sanne Ouburg, Winfried Tilanus
Version: 1.01
Date: 1 september 2025
Feature: Volledige versie, inclusief NDA check

Versiehistorie

Versie	Datum	Veranderingen
0.1	30 april 2025	Concept deel A
0.2	10 juni 2025	Volledige concept DPIA met feedback SURF en CACI op deel A verwerkt
0.9	18 juli 2025	Volledige concept DPIA met feedback SURF en CACI verwerkt
0.95	7 augustus 2025	Volledige concept DPIA met de input van CACI op de te nemen maatregelen verwerkt
1.0	1 september 2025	Volledige publieke DPIA met NDA-check van CACI verwerkt
1.01	5 september 2025	Updates in de statustabel verwerkt en oplegger toegevoegd

Inhoudsopgave

Oplegger DPIA Osiris – CACI B.V.

Beste lezer,

Vier jaar geleden heeft CACI haar strategische koers vastgelegd waarin privacy expliciet is benoemd als speerpunt. Niet als abstracte ambitie, maar als waarde die wij actief omarmen en verankeren in ons beleid en handelen.

Sindsdien hebben wij substantieel geïnvesteerd in het versterken van onze privacy-afdeling. We hebben onder andere een Functionaris Gegevensbescherming aangesteld, geïnvesteerd in professionele expertise van buitenaf, interne kennis en kunde verder opgebouwd, nog meer ingezet op bewustwording bij alle CACI-collega's en beleid ontwikkeld dat niet alleen op papier bestaat, maar daadwerkelijk wordt toegepast en continu verbeterd. Privacy is bij ons geen eenmalig project, maar een structureel onderdeel van onze organisatiecultuur.

CACI is intrinsiek gemotiveerd om de privacy van mensen centraal te stellen. Juist in een tijd waarin mondiale ontwikkelingen de urgentie van dataprotectie vergroten, blijven wij ons inzetten voor het beschermen van persoonsgegevens en het waarborgen van publieke waarden. De DPIA die nu voorligt, uitgevoerd door Privacy Company in opdracht van SURF, bevestigt dat onze inspanningen en investeringen hebben geleid tot een volwassen privacybeleid. We zijn trots op deze bevestiging, en zien het als een belangrijke mijlpaal in onze ontwikkeling. Tegelijkertijd erkennen we dat privacy nooit 'af' is. Het vraagt om voortdurende aandacht, reflectie en aanpassing.

Voor alle in de DPIA benoemde risico's die van toepassing zijn voor CACI implementeert CACI, waar nodig samen met de instellingen, adequate mitigerende maatregelen. Hiervoor is een samenhangend plan van aanpak opgesteld waarvan de uitvoering direct is gestart en de eerste resultaten al zijn opgeleverd.

Wij willen Privacy Company en SURF nadrukkelijk bedanken voor hun professionaliteit, grondige aanpak en de open, waardevolle gesprekken die hebben plaatsgevonden gedurende dit traject. Hun expertise, betrokkenheid en kritische blik hebben niet alleen bijgedragen aan de kwaliteit van deze DPIA, maar ook aan onze eigen reflectie en verdere ontwikkeling. Wij blijven met SURF en de betrokken onderwijsinstellingen samenwerken, in een gedeelde verantwoordelijkheid voor publieke waarden.

Mocht u vragen hebben aan of aanvullende informatie wensen van CACI, dan kunt u contact opnemen via privacy@caci.nl.

Met hartelijke groet,

Susanne Zuurendonk, Directeur CACI bv

Samenvatting

In opdracht van SURF heeft Privacy Company een Data Protection Impact Assessment (DPIA) uitgevoerd op Osiris. Osiris is een studenteninformatiesysteem (SIS) dat door CACI B.V. (hierna: CACI) wordt aangeboden. Osiris wordt in Nederland door mbo-instellingen, hbo-instellingen en wo-instellingen gebruikt. Osiris is een SaaS-oplossing met daarnaast een mobiele app. De mobiele app wordt door een substantieel deel van de onderwijsinstellingen die Osiris afnemen gebruikt.

Deze DPIA is gebaseerd op een combinatie van juridisch en technisch onderzoek. In het technische onderzoek zijn de daadwerkelijke verwerkingen van persoonsgegevens in kaart gebracht. Daartoe is gebruik gemaakt van een testomgeving van Osiris met behulp van Tilburg University (TiU). In de testomgeving zijn diverse scenario's uitgevoerd die bij het reguliere gebruik van Osiris logischerwijs voorkomen. Tijdens het testen is het netwerkverkeer onderschept. Daarna zijn voor verschillende typen gebruikers van de testaccounts inzageverzoeken ingediend. In aanvulling op het testen met scenario's is er ook direct informatie ingewonnen bij CACI.

Juridisch is geanalyseerd welke partijen zijn betrokken, welke rollen zij hebben en welke documentatie en overeenkomsten dit nader invulling geven. Tevens is beoordeeld voor welke doeleinden welke persoonsgegevens worden verwerkt bij het gebruik van Osiris en of de verwerkingen rechtmatig zijn.

In deze DPIA zijn in totaal twaalf initiële hoge risico's en één medium risico voor de rechten en vrijheden van betrokkenen geïdentificeerd. Daarvan zijn vier hoge risico's gerelateerd aan de mobiele app. Voor al deze risico's zijn maatregelen voorgesteld om de risico's te mitigeren, zodat alleen lage restrisico's overblijven. De risico's en maatregelen zijn soms van toepassing op CACI, als leverancier van Osiris, en soms op de onderwijsinstellingen als afnemers van Osiris.

Tabel 1: Risico-inventarisatie:

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.	Restrisico
1.	Instellingen gebruiken Osiris als administratie studentpsycholoog.	Gebruik Osiris niet als administratie of dossier van de studentpsycholoog, totdat CACI de beschreven maatregel heeft getroffen.	Maak Osiris geschikt voor gegevens die onder de WGBO vallen.	Laag
2.	Instellingen verwerken mogelijk BSN bij digitaal ondertekenen met DigID zonder wettelijke grondslag.	Maak waar mogelijk gebruik van andere methoden voor ondertekenen.	Wijs instellingen op de mogelijk onrechtmatige verwerking.	Laag

		Beoordeel de grondslag voor het gebruik van de BSN indien ondertekenen met DigID geactiveerd is.		
3.	Bestandsnamen in applicatielogs.		Wijzig de configuratie van de applicatielogs zodat bestandsnamen niet meer worden opgenomen.	Laag
4.	Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI).		Stel een procedure in om alle uitgegeven toegangsrechten regelmatig te toetsen en te beoordelen aan de hand van de actuele autorisatiematrix.	Laag
5.	Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens.	Neem zo weinig mogelijk bijzondere of gevoelige persoonsgegevens op in Osiris.	Optioneel: Bied de mogelijkheid aan om op veldniveau-encryptie toe te passen.	Laag
		Maak gebruik van de bestaande maatregelen, met name autorisatiemanagement, om de toegang tot bijzondere en gevoelige persoonsgegevens te beheren.		
6.	Onvoldoende governance koppelvlakken.	Richt de governance rond koppelvlakken adequaat in en controleer op naleving.		Laag
7.	Onvoldoende governance spiegeldatabase functionaliteit.	Indien gebruik gemaakt wordt van deze functionaliteit: richt adequate governance in om te voorkomen dat onbevoegde toegang of onrechtmatige verwerkingen ontstaan.		Laag

8.	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd.		Richt sleutelbeheer in conform NIST 800-57.	Laag
9.	Back-ups langer verwerkt dan nodig bij beëindigen contract.		Draag kopie database (via back-up) over aan instelling indien gewenst. Vernietig encryptiesleutel database (back-up) conform exitprocedure en verwerkers-overeenkomst.	Laag
Risico's verbonden aan de mobiele app				
10.	Onvoldoende transparantie over mobiele app.	Gebruik de informatie die CACI levert om gebruikers van de mobiele app adequaat te informeren.	Lever volledige informatie over de gegevensverwerkingen in de mobiele app.	Laag
11.	Mobiele app niet als 'side-load' beschikbaar.	Voer proportionaliteits- en subsidiariteitsbeoordeling uit op beschikbaar stellen mobiele app als 'side-load' en implementeer resultaten.	Stel op verzoek van de instelling de application programme kit (APK) beschikbaar.	Laag
12.	Pushberichten veroorzaken verwerking door Google en Apple.	Configureer pushberichten zo dat deze geen persoonsgegevens bevatten.	Faciliteer dat pushberichten zonder persoonsgegevens ingericht kunnen worden. Pas de inrichting van de applicatie aan zodat Unified Push gebruikt kan worden, indien aanwezig op het apparaat van de gebruiker.	Laag
13.	Verwerkersovereen komsten onvolledig m.b.t. mobiele app.	Vul de verwerkersovereenkomst aan met de verwerkingen	Vul de verwerkersovereen-komst aan met de verwerkingen die van	Laag

		die van toepassing zijn bij de mobiele app.	toepassing zijn bij de mobiele app.	

Een volledige conceptversie van deze DPIA is besproken met CACI. CACI heeft daarbij aangegeven al op een aantal punten maatregelen te treffen of getroffen te hebben. In onderstaande tabel is een overzicht van de status van de opvolging van de maatregelen opgenomen.

Tabel 2: Overzicht status maatregelen

#	Risico	Maatregelen CACI	Status
1.	Osiris als administratie studentpsycholoog.	Maak Osiris geschikt voor gegevens die onder de WGBO vallen, of zie maatregel onderwijsinstelling.	CACI bepaalt in overleg met instellingen of zij wensen dat Osiris geschikt wordt gemaakt voor gegevens die onder de WGBO vallen. ➔Uiterlijk Q4 2025: CACI neemt beslissing of bovenstaande gaat gebeuren en op welke termijn. Indien dit het geval is: ➔Uiterlijk Q2 2026: CACI stelt samen met de betrokken instellingen een planning op en implementeert de benodigde maatregelen.
2.	Verwerking van BSN bij digitaal ondertekenen met DigID heeft mogelijk geen wettelijke grondslag.	Wijs instellingen op de mogelijk onrechtmatige verwerking.	CACI heeft de instellingen die gebruik maken van digitale ondertekening geïnformeerd over de mogelijk onrechtmatige verwerking.
3.	Bestandsnamen in applicatielogs.	Wijzig de configuratie van de applicatielogs zodat bestandsnamen niet meer worden opgenomen.	CACI heeft de configuratie van de applicatielogs aangepast, zodat bestandsnamen niet meer worden opgenomen.
4.	Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI)	Stel een procedure in om alle uitgegeven toegangsrechten regelmatig te toetsen en te beoordelen aan de hand van de actuele autorisatiematrix.	CACI heeft deze procedure al gewijzigd. ➔Uiterlijk Q3 2025: CACI krijgt ISAE-audit om de implementatie van deze procedure te bevestigen.

5.	Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens.	Optioneel: Bied de mogelijkheid aan om op veldniveau encryptie toe te passen	Instellingen kunnen dit risico zelf naar een laag niveau brengen. CACI start in Q3 2025 echter ook een onderzoek naar de mogelijkheden van encryptie op veldniveau om instellingen te ondersteunen bij het mitigeren van dit risico.
6.	Onvoldoende governance koppelvlakken	-	Instellingen kunnen dit risico zelf naar een laag niveau brengen. CACI kan de instellingen wel adviseren, zodat ze een standaardwerkwijze kunnen toepassen.
7.	Onvoldoende governance spiegeldatabase functionaliteit	-	Instellingen kunnen dit risico zelf naar een laag niveau brengen. CACI kan de instellingen wel adviseren en ondersteunen bij het bijstellen van de spiegel naar wens (bijvoorbeeld door bepaalde gegevens niet mee te nemen).
8.	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd.	Richt sleutelbeheer in conform NIST 800-57.	➔Uiterlijk Q4 2025: CACI voert een analyse uit van de toepasselijkheid van NIST 800-57. ➔Uiterlijk Q2 2026: CACI implementeert de geïdentificeerde benodigde maatregelen op basis van NIST 800-57.
9.	Back-ups langer verwerkt dan nodig bij beëindigen contract.	Draag kopie database (via back-up) over aan instelling indien gewenst. Vernietig encryptiesleutel database (back-up) conform exitprocedure en verwerkersovereenkomst.	Het verwijderen van de encryptiesleutel en het overdragen van de kopie database zijn per direct mogelijk. ➔Uiterlijk Q3 2025: CACI neemt de beschreven maatregelen op in de exitprocedure, beschreven in de Standaard Dienstbeschrijving Osiris SaaS.
Risico’s verbonden aan de mobiele app			

10.	Onvoldoende transparantie over mobiele app.	Lever volledige informatie aan over de gegevensverwerkingen in de mobiele app.	➔Uiterlijk Q4 2025: CACI vult de verwerkersovereenkomst aan met de verwerkingen van persoonsgegevens die CACI als verwerker uitvoert ten behoeve van het leveren van de Osiris app.
11.	Mobiele app niet als ‘side-load’ beschikbaar	Stel op verzoek van de instelling de application programme kit (APK) beschikbaar.	CACI is per direct klaar om de APK te leveren op verzoek.
12.	Pushberichten veroorzaken verwerking door Google en Apple.	Faciliteer dat pushberichten zonder persoonsgegevens ingericht kunnen worden. Pas de inrichting van de applicatie aan zodat Unified Push gebruikt kan worden, indien aanwezig op het apparaat van de gebruiker.	CACI is per direct beschikbaar om te ondersteunen bij het inrichten van pushberichten zonder persoonsgegevens. Aanvullend start CACI in 2025 een onderzoek naar de mogelijkheid om het instellingen onmogelijk te maken persoonsgegevens op te nemen in pushberichten. ➔Uiterlijk Q4 2025: CACI doet onderzoek naar wat er nodig is om gebruikers in staat te stellen Unified Push te gebruiken voor de Osiris app. ➔Uiterlijk Q2 2026: CACI past de resultaten van het onderzoek toe en past de applicatie aan.
13.	Verwerkersovereenkomsten onvolledig m.b.t. mobiele app.	Vul de verwerkersovereenkomst aan met de verwerkingen die van toepassing zijn bij de mobiele app.	➔Uiterlijk Q4 2025: CACI vult de verwerkersovereenkomst aan met de verwerkingen van persoonsgegevens die CACI als verwerker uitvoert ten behoeve van het leveren van de Osiris app.

Inleiding

Osiris is een studenteninformatiesysteem (SIS) waarvan CACI B.V. (hierna: CACI) de leverancier is. CACI biedt Osiris aan als SaaS-applicatie. Een mobiele app, die zowel beschikbaar is voor zowel Android als iOS, is onderdeel van de SaaS-dienstverlening. Osiris wordt in Nederland door zowel mbo-instellingen, hbo-instellingen als wo-instellingen voor hoger onderwijs gebruikt. Een substantieel deel van deze instellingen biedt ook de Osiris-app aan haar studenten aan. SURF heeft deze DPIA door Privacy Company laten uitvoeren vanwege het grote aantal instellingen dat Osiris gebruikt, het grote aantal studenten en medewerkers dat daardoor met Osiris in aanraking komt en de gevoelige gegevens die in Osiris staan.

Osiris bestaat uit diverse functionele modules. Deze functionele modules zijn geïmplementeerd in een aantal 'applicaties'. Ten tijde van dit onderzoek was 'Osiris Aanmelding' een aparte applicatie. CACI is van plan om 'Osiris Aanmelding' te vernieuwen. Deze DPIA gaat echter uit van situatie zoals die ten tijde van het onderzoek is aangetroffen.

Centrale DPIA door SURF

SURF is de ict-coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen[1] en voert ten behoeve van de instellingen compliance assessments uit op leveranciers die technologische oplossingen aanbieden binnen de onderwijssector, waaronder DPIA's. De verwerkingsverantwoordelijke voor de verwerkingen die in deze DPIA beoordeeld worden is dus niet SURF, maar de instellingen die gebruik maken van Osiris. De DPIA is dan ook een 'centrale' of 'overkoepelende' DPIA, en biedt de instellingen een algemeen kader voor het beoordelen van gegevensbeschermingsrisico's binnen Osiris. Hiermee geeft de sector gezamenlijk invulling aan wettelijke verplichtingen.

Door het bundelen van expertise realiseert SURF kostenbesparing, kennisdeling en heeft SURF namens de onderwijs- en onderzoekssector een sterkere onderhandelingspositie richting de leveranciers ten aanzien van het nemen van eventuele mitigerende maatregelen. Dit levert voor de leverancier het voordeel op dat deze niet hetzelfde DPIA-proces met iedere klant uit de sector hoeft te doorlopen en in één keer maatregelen kan implementeren die (hoge) risico's voor de hele sector mitigeren. De AP heeft de kracht van de samenwerking van de onderwijs- en onderzoeksinstellingen via SURF onderschreven en benadrukt dat dit wijze bijdraagt aan het beschermen van de persoonsgegevens in het onderwijs en onderzoek.[2]

In deze centrale DPIA wordt onderzocht hoe de persoonsgegevens van studenten en medewerkers van de instellingen binnen Osiris worden verwerkt, welke centrale afspraken er zijn gemaakt over de verwerkingen, welke risico's er bestaan en welke maatregelen genomen kunnen worden om deze risico's te beperken. De DPIA biedt een startpunt, maar is op zichzelf staand niet voldoende om als verwerkingsverantwoordelijke aantoonbaar te voldoen aan de AVG. Het door de onderwijsinstelling uitvoeren van een lokale DPIA is noodzakelijk om het eigen gebruik van Osiris in kaart te brengen, de eigen grondslagen vast te stellen en om organisatiespecifieke risico's te beoordelen. Een lokale DPIA biedt de nodige diepgang en

[1] Overzicht leden van SURF | SURF.nl.

[2] Zie ook: Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6,
https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

inzichten op specifieke omstandigheden of organisatorische kenmerken die deze centrale DPIA niet kan leveren.

Scope van het onderzoek

Deze DPIA betreft de SaaS-applicatie van Osiris en de Osiris mobiele app voor zowel Android als iOS. Binnen scope van deze DPIA zijn de volgende functionele modules:

- Osiris Docent/Begeleider
- Osiris Student
- Osiris Aanmelding
- Osiris Studievolg
- Osiris Inschrijving
- Osiris Zaak

Osiris wordt zowel bij mbo's, hogescholen en universiteiten gebruikt. De werkprocessen van de mbo's wijken in een aantal opzichten sterk af van die van de hogescholen en universiteiten. Doordat deze DPIA is uitgevoerd bij een universiteit, was het niet mogelijk om een aantal van de processen van de mbo's te testen. In hoofdstuk 2 en paragraaf 4.1 van de Technische Appendix is te vinden welke processen zijn getest. De conclusies van deze DPIA zijn echter wel te generaliseren naar de mbo's.

De PlanApp, Osiris Debiteur en Osiris Cursusinvoer zijn buiten scope van deze DPIA.

De DPIA is gebaseerd op een combinatie van juridisch en technisch onderzoek.

Testmethodiek

Voor deze DPIA is een aantal tests uitgevoerd. Voor deze tests werden een aantal scenario's doorlopen. Bij elk scenario zijn zowel de gegevens die zichtbaar waren in het scherm als de gegevens die tussen de browser of app en de servers uitgewisseld werden vastgelegd. De tests zijn samengesteld met de volgende uitgangspunten:

- De tests moeten alle technische modules van Osiris bestrijken die in scope zijn
- De tests moeten de meest gevoelige gegevens in Osiris bestrijken
- De tests moeten de basisprocessen van Osiris bestrijken
- De tests moeten inzage geven in koppelingen die cliënt side plaatsvinden, zoals de authenticatie

Op basis van deze uitgangspunten is in samenwerking met Tilburg University (hierna: TiU) een testscript opgesteld. Dit script is opgenomen in de Technische Appendix.

De volgende rollen zijn gebruikt bij het testen:

1. Student
2. Docent
3. Immigratie-officer
4. Decaan
5. Ondersteuner examencommissie
6. Administratie
7. Onderwijscoördinator
8. Studentenpsycholoog

De tests zijn uitgevoerd in de testomgeving van TiU. Voor het uitvoeren van de tests zijn een aantal accounts met verschillende rollen in Osiris aangemaakt. De accounts zijn gekoppeld aan bestaande personen. Privacy Company heeft na het testen op basis van de accounts drie inzageverzoeken ingediend bij TiU.

Tijdens het testen is het netwerkverkeer tussen de browser en de mobiele apps onderschept. Dit verkeer is na afloop geanalyseerd. Het verloop van de testen en de volledige resultaten daarvan staan in de Technische Appendix. In de hoofdtekst worden waar relevant de resultaten daarvan weergegeven.

In dit rapport staan de resultaten uit de testen en de juridische analyse van de bevindingen uit het onderzoek. Bij dit rapport hoort een Technische Appendix met een gedetailleerde weergave van de testresultaten. Deze Technische Appendix is op verzoek beschikbaar bij SURF.

Model

Deze DPIA is gebaseerd op de model DPIA Rijksdienst. Dit model sluit goed aan op de werkzaamheden van onderwijs- en onderzoeksinstellingen, die ze in het publieke belang uitvoeren. Aangezien dit een centrale DPIA is, zijn er waar nodig wijzigingen aangebracht in de structuur van het originele model.

Het model bestaat uit vier onderdelen. Onderdeel A behandelt de feiten van de gegevensverwerkingen. Onderdeel B beoordeelt de rechtmatigheid van de behandelde feiten uit onderdeel A. Onderdeel C gaat over risico’s voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico’s aan te pakken.

Deel A: Beschrijving van het systeem

1 Beschrijving van de verwerkingen

Osiris is een studentvolgsysteem dat door ongeveer 65 onderwijsinstellingen in Nederland gebruikt wordt en afkomstig is van het bedrijf CACI. Osiris kent meerdere functionele applicaties waarmee instellingen verschillende (bedrijfs)processen kunnen bijhouden. Gelet op de studentpopulaties van Nederlandse onderwijsinstellingen, worden er via Osiris persoonsgegevens van een groot deel van de Nederlandse studentenpopulatie verwerkt. De aard van de gegevens die binnen Osiris verwerkt kunnen worden loopt uiteen van 'reguliere' persoonsgegevens tot bijzondere persoonsgegevens zijn. CACI biedt Osiris aan als SaaS-dienstverlening, host deze dienstverlening van Osiris volledig in het datacentrum van Interconnect en beheert de dienstverlening in zijn geheel.

Voor deze DPIA is gekeken naar de wijze van gebruik door Tilburg University (TiU). De beschrijvingen in dit rapport zijn zoveel mogelijk vertaald naar de generieke situatie. Op sommige punten staat extra toelichting over de specifieke werkwijze van TiU.

De verschillende functionele modules binnen Osiris zijn gericht op gebruikersgroepen, zoals docenten of studenten. In deze DPIA wordt gekeken naar de volgende functionele modules:

- Osiris Docent/Begeleider
- Osiris Student
- Osiris Aanmelding
- Osiris Studievolg
- Osiris Inschrijving
- Osiris Zaak

De PlanApp, Osiris Debiteur en Osiris Cursusinvoer zijn buiten scope van deze DPIA.

1.1 Architectuur en onderdelen

Osiris is een single-tenant oplossing, wat betekent dat elke instelling een eigen afgescheiden omgeving, installatie en database heeft. Op architectuurniveau bestaat Osiris uit verschillende applicaties. Iedere applicatie wordt gebruikt door verschillende functionele modules. De verschillende applicaties binnen een klantomgeving verbinden allemaal naar dezelfde centrale Oracle-database van die klantomgeving. De applicaties hebben allemaal een eigen front-end en gebruiken daarvoor verschillende frameworks (standaard software bouwblokken).

De software-stack van Osiris SaaS ziet er als volgt uit:

- Virtualisatie platform, netwerk en firewall; deze worden geleverd en beheerd door Interconnect .
- Virtuele machines (database-, applicatie- en webservers); deze worden beheerd door CACI.
- Oracle Linux.
- Oracle Database; de database voert alle business-logica van Osiris uit, in de vorm van 'procedures'.
- Applicaties; de verschillende applicaties maken gebruik van verschillende frameworks voor het creëren van een user interface. Deze frameworks worden deels als software door Oracle aan CACI geleverd en zijn deels open source.
- Diverse virtuele machines voor management en monitoring taken.

Tabel 3: Applicaties van Osiris

Applicatie	Doelgroep	Functionele Modules (in scope)	Framework
Osiris Basis	Administratie, poweruser	Inschrijving, Studievolg en Zaak	Oracle ADF + JHeadstart voor generatie schermen
Osiris Docent/ Begeleider	Docenten en begeleiders van studenten, selfservice	Student, Studievolg en Zaak	Oracle ADF
Osiris Student	Studenten, selfservice Zowel web-based als mobile app	o.a. Student, Zaak	Ionic 8 + Angular 18 - UI Spring / camel - service routing Oracle ORDS - webservices
Osiris Aanmelding	Studenten, selfservice	Aanmelding	Oracle UIX

Osiris Basis is de kernapplicatie voor de administratie. Hiermee kan de administratie van de onderwijsinstelling (en andere powerusers) alle gegevens rond onderwijs en studenten onderhouden. Osiris Basis ontsluit alle gegevens die in de database zitten.

Osiris Basis is gebouwd met het Oracle Application Development Framework (ADF) en deels met JHeadstart, een framework dat automatisch user interfaces bij de tabellen genereert. Waar nodig vult CACI dit aan met logica, geprogrammeerd in Java.

Osiris Docent/ Begeleider is een applicatie waarmee docenten en begeleiders zelf verschillende taken kunnen uitvoeren. De applicatie is in technische zin één geheel, maar beslaat verschillende functionele modules, waaronder Student, Resultaten en Zaak.

De userinterface van Osiris Docent/ Begeleider is geheel in Oracle ADF geïmplementeerd.

Osiris Student is een applicatie waarmee studenten zelf verschillende taken kunnen uitvoeren. De applicatie is beschikbaar als webapplicatie en, optioneel, ook als mobiele app.

Osiris Student is gebouwd met een framework dat zowel een webapplicatie als een mobiele applicatie kan genereren. Zowel de webapplicatie als de mobiele applicatie verbinden via een aparte interface met de database.

Osiris Aanmelding is de selfservice applicatie voor studenten, waarmee ze zich kunnen aanmelden voor een opleiding of waarmee ze aanvullende informatie rond hun aanmelding kunnen vastleggen en bekijken. Osiris Aanmelding is gebouwd met het Oracle User Interface XML (UIX) framework.

1.2 Functionele modules

Deze modules kunnen, afhankelijk van wat de onderwijsinstelling ingekocht heeft, aan- of uitgezet worden. De hier besproken modules worden door veel onderwijsinstellingen gebruikt en verwerken persoonsgegevens.

1.2.1 Osiris Docent/Begeleider

Osiris Docent en begeleider biedt de volgende functionaliteiten voor docenten:

- Resultaten invoeren
- Resultaten inzien
- Resultaten wijzigen
- Beoordelingsformulieren verwerken
- Resultaten elektronisch ondertekenen
- Presentielijsten opvragen
- Inzien van vrijstellingen
- Pasfotolijsten opvragen (indien de instelling de pasfotofunctie gebruikt)
- Roosterinformatie opvragen (indien de instelling de roostermodule gebruikt)

Osiris Docent ondersteunt verschillende workflows voor het goedkeuren van cijfers. In tegenstelling tot de meeste andere instellingen, voert bij TiU niet de docent maar de administratie de door de student behaalde cijfers in. Tijdens het testen is deze afwijkende workflow gevolgd.

1.2.2 Osiris Student

Osiris Student biedt onder meer de volgende functionaliteiten voor studenten:

- Overzicht geven van de behaalde resultaten
- Behaalde resultaten vergelijken met het (individuele) studiecontract/ examenprogramma
- Inschrijven op cursussen of minors
- Zoeken door het onderwijsaanbod
- Weekrooster opvragen
- Aanvragen doen (indien de instelling de module Zaak gebruikt)
- Adreswijzigingen doorgeven

1.2.3 Osiris Aanmelding

Osiris Aanmelding biedt onderwijsinstellingen de mogelijkheid om een aanmeldprocedure in te richten voor studenten die niet via Studielink aangemeld worden. Denk bijvoorbeeld aan studenten van een internationaal uitwisselingsprogramma, contractonderwijs, etc. Zie 1.3 Het aanmeldproces voor meer informatie. Ook is het mogelijk om via Osiris Aanmelding een vervolgproces op de aanmelding via Studielink te doorlopen, bijvoorbeeld voor plaatsing en selectie.

1.2.4 Osiris Studievolg

Osiris Studievolg biedt de mogelijkheid om zowel onderwijsgerelateerde als studentgebonden gegevens op een gestructureerde wijze vast te leggen. Daarnaast ondersteunt de module bij het ontwerpen en beheren van studieplannen en onderwijsprogramma's, zowel vanuit

organisatorisch perspectief als vanuit de student zelf. Op basis van het beschikbare onderwijsaanbod kunnen op maat gemaakte studieprogramma's worden samengesteld.[3]

Osiris Studievolg biedt de volgende functionaliteiten:

- Beheren van documenten over een student of opleiding, inclusief het instellen van bewaartermijnen van de documenten
- Het ontwerpen en beheren van studieplannen en onderwijsprogramma's
- Het definiëren van cursusaanbod en examenprogramma's
- Het uitbrengen van een bindend studieadvies

1.2.5 Osiris Inschrijving

Osiris Inschrijving begeleidt het inschrijvingsproces van een student, van de eerste aanmelding via Studielink tot een volledige actieve inschrijving. Tussen deze twee momenten zitten verschillende tussenstappen. Zie 1.3 Het aanmeldproces voor meer informatie.

1.2.6 Osiris Zaak

Een onderwijsinstelling kan in Osiris Zaak administratieve processen definiëren die vervolgens binnen Osiris op een gestructureerde manier afgehandeld kunnen worden. Denk daarbij aan zaken als:

- Ondersteuning van de examencommissie in geschillen met een student
- Verzoeken om vrijstelling
- Aanvragen van voorzieningen
- Opleggen van sancties

1.3 Het aanmeldproces

De meeste studenten melden zich via Studielink aan (en af) voor de universiteiten en hogescholen. Bij mbo's verloopt dit proces via CAMBO. Studielink is een door de instellingen voor hoger onderwijs bekostigde stichting die het aanmeldproces zo soepel mogelijk wil laten verlopen. Het aanmeldproces volgt uit de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW). Studielink vervult de volgende taken in het aanmeldproces:

- Verifiëren van de persoonsgegevens aan de hand van de Basisregistratie Personen (BRP)
- De aanmelding doorgeven aan DUO
- Controleren of de student aan de wettelijke aanmeldingseisen voldoet
- Aanmeldingen doorgeven aan de onderwijsinstelling
- Bij numerus fixus studies: nadat de onderwijsinstelling de volgorde heeft vastgesteld, de formele toelating doorgeven
- Het verzamelen van machtigingen voor het innen van het collegegeld
- Voor sommige onderwijsinstellingen: het faciliteren bij het aanvragen van een verblijfsvergunning. Hiervoor heeft studielink een koppeling met de IND.

Osiris heeft een directe koppeling met Studielink. Via deze koppeling komt in de meeste gevallen de eerste aanmelding van de student binnen. Na de eerste aanmelding heeft de procedure een aantal stappen voordat de student volledig ingeschreven is. Dat gaat over zaken als voldoen aan de toelatingseisen (ook als de student bijvoorbeeld pas na de inschrijving het diploma behaalt of als het om buitenlandse diploma's gaat), het vaststellen van de volgorde bij een numerus fixus

[3] https://www.caci.nl/osiris/

opleiding, de betaling van het collegegeld, het aanmaken van accounts op de systemen van de onderwijsinstelling en het daadwerkelijk inschrijven voor een cursus. Deze procedure kan per onderwijsinstelling verschillen. Binnen Osiris Inschrijving, kan de onderwijsinstelling deze procedure vastleggen. Indien gewenst kan de onderwijsinstelling binnen Osiris Aanmelding de interactie met de student tijdens dit proces, bijvoorbeeld rond de toelating tot numerus fixus opleidingen, uitvoeren.

Als er voor een student een verblijfsvergunning aangevraagd moet worden, dan kan een onderwijsinstelling ervoor kiezen om dat ook via Studielink te laten verlopen of om dat proces zelf uit te voeren. In dat laatste geval meldt de onderwijsinstelling bij succesvolle inschrijving de student bij Studielink aan. Ook deze procedure kan de onderwijsinstelling binnen Osiris Aanmelding vormgeven. Voor deze workflow is onder andere een kopie van het paspoort nodig.

Contractonderwijs valt niet onder de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW). Het aanmelden daarvoor vindt buiten Studielink plaats. Indien gewenst kan een onderwijsinstelling het inschrijven voor contractonderwijs via Osiris Aanmelding laten verlopen.

TiU gebruikt Osiris Aanmelding voor contractonderwijs en voor het inschrijven van studenten voor wie een verblijfsvergunning aangevraagd moet worden. Tijdens het testen is een scenario met een student voor wie een verblijfsvergunning aangevraagd moet worden uitgevoerd, zodat het testen ook Osiris Aanmelding zou beslaan.

1.4 Authenticatie en autorisatie

Osiris maakt, voor zowel de studenten als de medewerkers, gebruik van de authenticatieserver van de onderwijsinstelling. Als stap in het aanmeldingsproces, worden de gegevens over aangemelde studenten uit Osiris doorgegeven aan de authenticatieserver van TiU. Vanaf dat moment kan de student, via de authenticatieserver, inloggen op Osiris. Om in te loggen stuurt Osiris de webbrowser waarmee Osiris geopend is, door naar de authenticatieserver van de onderwijsinstelling om via het oAuth protocol te authenticeren. De communicatie tussen Osiris en de authenticatieserver verloopt via het SAML-protocol. Indien de student of medewerker al ingelogd is, maakt deze workflow direct inloggen met Single Sign-on (SSO) mogelijk, anders doorloopt de student of de medewerker de authenticatieflow van de instelling. In de app voor studenten wordt deze interactie uitgevoerd vanuit een in-app browser. De authenticatieserver zelf is buiten scope van deze DPIA.

Osiris biedt de mogelijkheid om een fijnmazige autorisatiematrix in te stellen. Deze autorisaties zijn zowel per rol als per faculteit, afdeling, cursus of student in te stellen. Het inregelen en onderhouden van deze autorisaties is de verantwoordelijkheid van de onderwijsinstelling. Bij de eerste implementatie begeleidt CACI de instellingen bij het instellen ervan. Vervolgens is het aan de onderwijsinstelling zelf om de autorisaties te onderhouden.

TiU maakt onderscheid tussen 76 verschillende rollen en taken en heeft deze rollen uitgewerkt in een uitgebreid rollenboek. Tijdens het testen bleek deze aanpak adequaat te zijn: de verschillende medewerkers konden bij de gegevens die ze nodig hadden maar bij niets meer dan dat.

1.5 Koppelingen

Osiris biedt een groot aantal koppelingen met andere systemen en daar bovenop verschillende mogelijkheden voor de onderwijsinstellingen om eigen koppelingen te definiëren. In de Technische Appendix is een overzicht opgenomen van alle standaard koppelingen en welke van die koppelingen binnen of buiten scope van deze DPIA zijn.

De testomgeving bij de TiU had drie niet standaard koppelingen geïmplementeerd:

- Roosterview: roosterprogramma. Tijdens het testen was de TiU bezig om een embedded webpagina met gegevens van roosterview toe te voegen aan de site.
- Canvas: leeromgeving.
- Succesfactors: personeelszaken.

Deze drie koppelingen zijn niet getest en zijn buiten scope van deze DPIA.

1.5.1 Studielink

Studielink is een samenwerking tussen de instellingen voor hoger onderwijs. Het doel van Studielink is om het aanmeldproces te stroomlijnen. Daarvoor bieden ze een centraal portaal voor aanmeldingen en koppelingen met studentinformatiesystemen zoals Osiris, met DUO en met de Basisregistratie Personen.

In de koppeling tussen Studielink en Osiris is de datastroom voor het grootste deel van Studielink naar Osiris. Bij studenten die niet via Studielink kunnen aanmelden, vooral studenten uit een land buiten de EU, loopt de datastroom ook de andere kant op. Verder stuurt Osiris updates, zoals bevestigingen van betalingen van collegegeld en adreswijzigingen naar Studielink.

Op twee uitzonderingen na, gaan de met Studielink uitgewisselde gegevens over studenten. Als de onderwijsinstelling de verificatie van de identiteit van een student uitvoert, dan moet de onderwijsinstelling de naam van de medewerker die de verificatie uitvoert doorgeven en als een student overlijdt, en de onderwijsinstelling meldt dat, dan moet de onderwijsinstelling doorgeven welke medewerker die melding doet.

De gegevens die via de koppeling tussen Osiris en Studielink uitgewisseld worden zijn:

- Identificerende gegevens: BSN, een door studielink toegekend persoonsnummer, studentnummer van de onderwijsinstelling, samengestelde naam.
- Personalia: Volledige naam, adresgegevens, contactgegevens, correspondentietaal, geslacht (volgens BRP), geboorteplaats, geboorteland, geboortedatum.
- Verblijfsstatus: eerste en tweede nationaliteit, gegevens verblijfsvergunning, land waar de student zich bevindt indien de student niet meer in Nederland verblijft.
- Gegevens over de inschrijving: studiekeuzes, toelating tot studies met een capaciteitsbeperking, updates over de inschrijving.
- Gegevens over de vooropleiding: diploma's, examenvakken, behaalde resultaten.
- Gegevens over de betaling van collegegeld: machtigingen, betaaltermijnen, of het collegegeld voldaan is.
- Of de student overleden is.

Een volledig overzicht van de uitgewisselde gegevens staat in de Technische Appendix.

1.5.2 IND

Osiris kan het proces voor een aanvraag van een verblijfsvergunning bij de Immigratie en Naturalisatie Dienst (IND) begeleiden. Daarvoor communiceert Osiris met de IND. De

communicatie tussen Osiris en de IND verloopt via Studielink. Deze berichtenstromen kunnen twee kanten op gaan. De volgende type gegevens kunnen uitgewisseld worden:

- Gegevens van de aanvraag: opleiding, verblijfsduur in Nederland, betaling, status van de aanvraag.
- Gegevens van de student: Naam, adres, contactgegevens, gegevens rond geboorte, reisdocument, identificerende nummers.

Een volledige beschrijving van deze gegevens staat in de Technische Appendix.

1.5.3 Digitaal ondertekenen

Osiris kent twee typen van digitaal ondertekenen. Het eerste type is het ondertekenen van cursusresultaten. Bij die manier van ondertekenen authentiseert de docent een keer extra bij de authenticatieserver van de onderwijsinstelling om vast te stellen dat de resultaten inderdaad door de docent zijn ingevoerd.

Bij andere workflows, kunnen documenten via een API bij een externe dienst ondertekend worden. Alleen mbo-instellingen gebruiken deze workflow. De ondertekende documenten worden daarna weer onderdeel van een workflow binnen Osiris. Osiris en de externe dienst ondersteunen verschillende manieren van ondertekenen, een van deze manieren is ondertekenen met DigID. Ondertekenen met DigID wordt op een beperkt aantal mbo-instellingen daadwerkelijk gebruikt.

De API-documentatie[4] van Osiris geeft aan dat de volgende gegevens worden uitgewisseld met de dienst voor het ondertekenen als van ondertekenen met de BSN gebruik gemaakt wordt:

- De te ondertekenen documenten
- Gegevens van de ondertekenaar, inclusief BSN en contactgegevens
- De ontvanger van de documenten
- Opleiding, instelling en vestiging

Voor het ondertekenen met DigID heeft de ondertekendienst het BSN van de ondertekenaar nodig. Alleen als daadwerkelijk gebruik wordt gemaakt van DigID als ondertekenmethode, wordt het BSN van Osiris doorgegeven aan de ondertekendienst.

Geen van de twee manieren van ondertekenen werden door TiU gebruikt. Het ondertekenen is daarom niet getest.

1.5.4 Erasmus Without Paper

Erasmus Without Paper (EWP) is een systeem voor gegevensuitwisseling tussen de onderwijsinstellingen die deelnemen aan het Europese Erasmus uitwisselingsprogramma. Het systeem is peer-to-peer tussen de onderwijsinstellingen opgezet en volgt de uitwisselingsovereenkomsten tussen de instellingen. De volgende persoonsgegevens, die zowel studenten als betrokken medewerkers kunnen betreffen, worden via EWP uitgewisseld:

- Naam, geboortedatum, gender, contactgegevens
- Nationaliteit, nationale identificatienummer
- Bij welke uitwisseling de persoon betrokken is of deelneemt
- Rol binnen de uitwisseling

[4] Documentatie json Open API Koppelvlakken.

Het volledige datamodel van EWP is opgenomen in de Technische Appendix. De omschrijving van het datamodel specificeert niet of het 'nationale identificatienummer' een door de staat uitgegeven identificatienummer moet zijn of een uniek nummer dat bijvoorbeeld door een onderwijsinstelling of door samenwerkende onderwijsinstellingen wordt uitgegeven. Osiris gebruikt voor EWP de ESI (European Student Identifier, ook bekend als global id). De ESI wordt samengesteld uit verschillende gegevens, waaronder het studentnummer. Deze gegevens worden samengevoegd en worden vervolgens versleuteld. Hierdoor ontstaat een reeks die wel uniek is voor de student, maar waaruit de gegevens waarmee het is opgebouwd niet zijn te herleiden.

1.5.5 EduXchange

EduXchange is een koppeling die studenten de mogelijkheid biedt om inzicht te krijgen in het vak- en minoraanbod van andere onderwijsinstellingen, zich hiervoor in te schrijven en de behaalde resultaten terug te koppelen naar de eigen onderwijsinstelling.[5] De gegevensuitwisseling verloopt via de SURF EduHub en maakt gebruik van het centrale EduID. De volgende persoonsgegevens over studenten worden via eduXchange uitgewisseld:

- Naam, geboortedatum, nationaliteit, gender, contactgegevens, voorkeurstaal
- Onderwijsinstelling waarmee de student verbonden is
- Vak of cursus die gevolgd wordt
- Resultaten

1.5.6 Integratiecomponenten

Osiris biedt standaard integratiecomponenten waarmee onderwijsinstellingen gegevens kunnen uitwisselen met externe systemen, zoals een roostersysteem of een financieel systeem. Met deze componenten kunnen twee soorten interfaces worden geconfigureerd. De ene interface voorziet in pull verkeer, waarbij een extern systeem het initiatief neemt en zelf informatie uit Osiris opvraagt of bijwerkt. De andere interface voorziet in push verkeer, waarbij het Osiris het initiatief neemt voor de gegevensuitwisseling, bijvoorbeeld als er binnen Osiris een update is voor een student.

Beide interfaces zijn flexibel configureerbaar. Onderwijsinstellingen kunnen bepalen welke gegevens worden gedeeld en onder welke voorwaarden. Hiervoor biedt Osiris verschillende mechanismen, zoals:

- Via standaard filters van Osiris.
- Via eigen database query code (SQL)
- Via eigen voorwaarden ("alleen tonen als …")
- Via het uitsluiten van bepaalde kolommen (bijvoorbeeld 'BSN')
- Via de ingeregelde permissies

Toegang tot deze interfaces is afgeschermd met authenticatie. Deze interfaces zijn via userinterface te configureren.

Voor het realiseren van de interfaces biedt Osiris de volgende integratiecomponenten:

[5] https://wiki.surfnet.nl/spaces/EDX/pages/128126952/eduXchange+hoe+werkt+het

1.5.6.1 System Services

Dit component biedt een REST/JSON-interface waarmee externe systemen op aanvraag gegevens kunnen opvragen of bijwerken. Deze 'listener'-component wacht op inkomende servicecalls van externe systemen (pull-interface).

1.5.6.2 Eventbroker

Dit component werkt op basis van een event-driven architectuur (push-interface). Het component zoekt actief contact met het gekoppelde externe systeem, als er een bepaald event plaatsvindt binnen Osiris of op vaste tijdstippen. Deze integratie ondersteunt verschillende formaten (XML, JSON, FORM, SOAP). Het biedt ook mogelijkheden om de berichten volgens een bepaalde template vorm te geven. Het heeft optionele mechanismes om dubbele berichten uit te filteren of om opnieuw te proberen als ontvangende partij niet bereikbaar is.

1.5.7 Databasereplicatie

Osiris biedt de onderwijsinstellingen de mogelijkheid om een (read-only) constante replicatie van de database te maken naar een eigen server (zie ook 1.6 Opslag). In dat geval is de complete database beschikbaar op een server die door de onderwijsinstelling beheerd wordt. Onderwijsinstellingen kunnen dan de gegevens direct vanaf deze server bevragen, via SQL (een database query language), of via een tool als PowerBI. Daarnaast biedt dit ook de mogelijkheid om de gegevens uit de database, via een 'pipeline' door te sturen naar een datalake, een systeem waarmee gegevens uit verschillende systemen verzameld, gecombineerd en verwerkt kunnen worden. Deze gegevens kunnen als basis dienen voor bepaalde werkprocessen, maar kunnen ook met tools als PowerBI geanalyseerd worden.

1.6 Opslag

Osiris heeft per instelling een eigen database. Een instelling heeft doorgaans meerdere installaties, een productieomgeving en verschillende testomgevingen. Deze database wordt uitgevoerd op een backend server waarvan de software door Oracle geleverd is en die gehost is bij Interconnect. De business-logica van Osiris wordt uitgevoerd als procedures in de database. Om de data uit te kunnen lezen zonder dat de hoofddatabase te zwaar belast wordt, kan Osiris de database constant repliceren naar een (tweede) server waar de data kunnen worden uitgelezen met alleen leesrechten. De tweede server is optioneel en alleen beschikbaar als de instelling een query-database afneemt.

De database bevat drie typen tabellen:

- Tabellen met tijdelijke gegevens. Deze gegevens zijn een tussenresultaat bij een verwerking. Deze gegevens worden bij de eerstvolgende clean-up gewist, doorgaans binnen enkele uren.
- Normale tabellen. Bij deze tabellen kan de onderwijsinstelling de bewaartermijn instellen.
- 'Historietabellen'. Van deze tabellen houdt de database alle mutaties bij (INSERT, UPDATE, DELETE) in een losse historietabel behorende bij de basistabel. Dit betekent dat bij een standaard delete uit de basistabel, de verwijderde rij wel nog wordt bewaard in de bijbehorende historietabel. Het clean-up proces bij het opschonen van de database verwijdert ook alle historiegegevens waarvan de bewaartermijn is overschreden.

Van de volgende gegevens houdt Osiris historietabellen bij:

- Personalia van de student, inclusief geboortedatum en plaats, nationaliteit, verblijfsstatus, e-mailadressen en telefoonnummers.
- Status van de inschrijving van de student voor een opleiding, inclusief vooropleiding.
- Status van de inschrijving voor een cursus.
- Toetsuitslagen.
- Aanvragen voor voorzieningen in verband met een beperking.
- Verzuimmeldingen.
- Alle gegevens rond een ‘zaak’, exclusief geüploade documenten.

Daarnaast houdt Osiris historietabellen bij voor modules die niet binnen de scope van deze DPIA vallen.

1.7 Hosting

CACI host Osiris op virtuele machines. De onderliggende fysieke machines staan in een datacentrum van Interconnect in Nederland. De virtuele machines hebben Oracle Linux als besturingssysteem en een Oracle Enterprise Database.

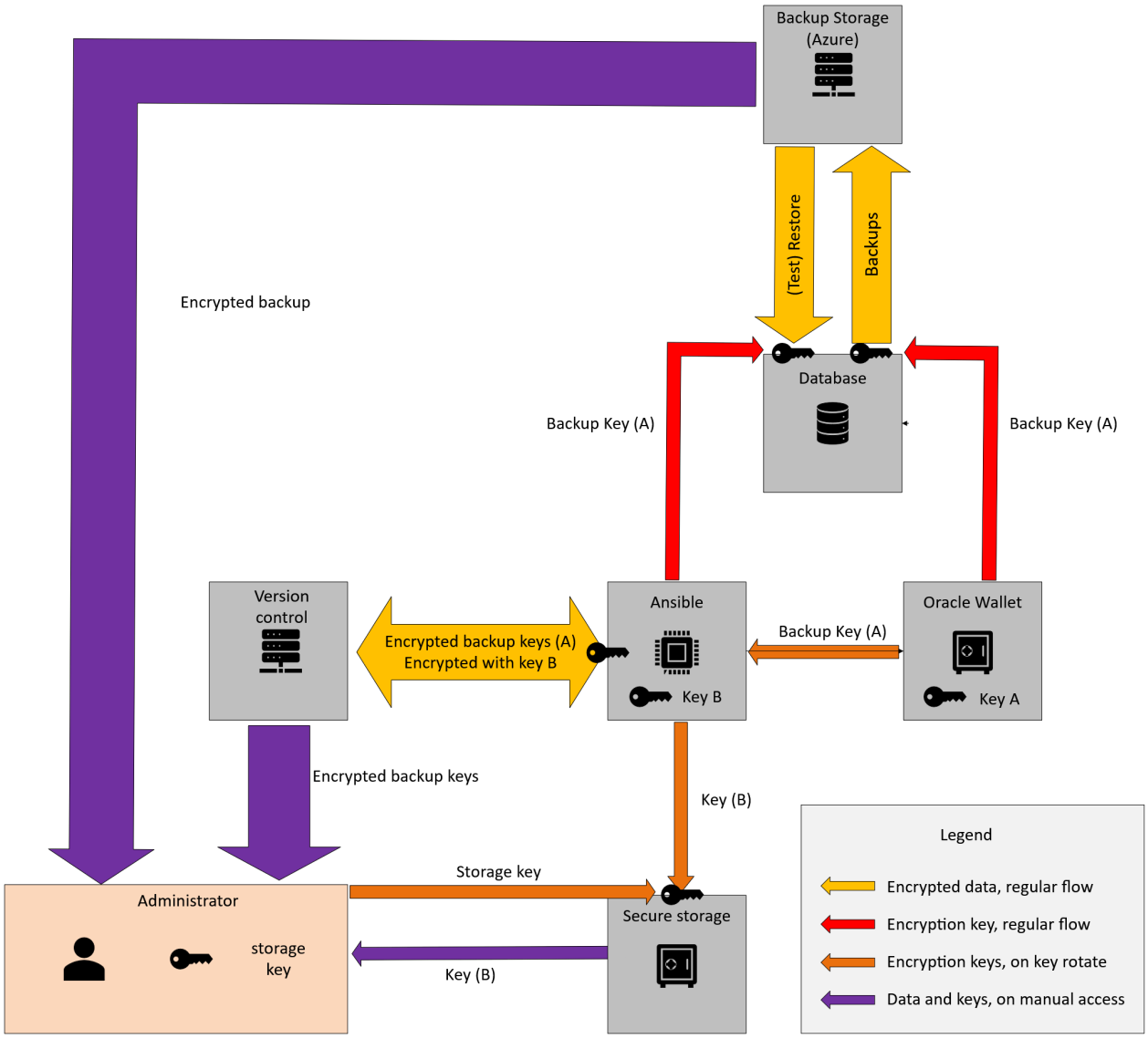
1.8 Beveiliging

Interconnect verzorgt een firewall in de externe verbindingen van de virtuele servers. Deze firewall filtert op IP-adres en type verkeer (op poort basis) en stuurt het verkeer ongewijzigd en zonder te ontsleutelen door naar de virtuele infrastructuur van Osiris. Daardoor ziet Interconnect alleen de IP-adressen van de mensen die gebruik maken van Osiris, maar Interconnect kan niet herleiden welke functies van Osiris aangeroepen worden en wat de inhoud van het verkeer is. Het verkeer wordt pas in de virtuele infrastructuur van Osiris ontsleuteld. Doordat de firewall het verkeer naar Osiris doorstuurt vanaf het eigen interne IP-adres, ziet Osiris niet de IP-adressen van de mensen die contact hebben met Osiris.

Binnen SaaS-oplossingen zijn doorgaans verschillende niveaus van encryptie mogelijk: op veldniveau, op database-niveau via Transparent Data Encryption (TDE), en op diskniveau. In Osiris past CACI momenteel uitsluitend diskniveau-encryptie toe. TDE wordt bij één instelling toegepast, terwijl veldniveau-encryptie niet is geïmplementeerd.

CACI versleutelt alle database back-ups. Voor de versleuteling gebruikt CACI het AES256 algoritme, een algoritme dat aan de courante veiligheidsstandaarden voldoet. Het AES256 algoritme is symmetrisch, wat betekent dat zowel het versleutelen als het ontsleutelen met dezelfde sleutel gebeurt. Voor het sleutelbeheer, maakt CACI gebruik van de ‘Oracle Secured Wallet’ software. Deze software is ook gehost bij Interconnect. Bij het terugzetten van een back-up, maakt CACI gebruik van Ansible. Ansible is een systeem voor geautomatiseerd beheer van een serverpark. Ansible draait binnen de infrastructuur van CACI.

Figuur 1: Encryptie back-ups



CACI maakt een back-up van de sleutels door deze met weer een andere sleutel te versleutelen en deze versleutelde sleutel in een versiebeheersysteem op te nemen. De Oracle Secured Wallet levert sleutel A aan de database. Sleutel A is de sleutel waarmee de back-up versleuteld wordt. De Secured Wallet stuurt sleutel A ook door naar Ansible. Ansible beheert een eigen sleutel, sleutel B. Deze sleutel B is beveiligd door het secret management van Ansible. Ansible versleutelt met sleutel B de sleutels A die het ontvangt van de Secured Wallet en stuurt deze naar de version control als opslag. Ansible stuurt een kopie van de sleutel B naar een beveiligde opslag intern bij CACI. Deze beveiligde opslag is beveiligd met een storage key die maar een enkele beheerders van CACI hebben.

Voor een (test) restore, haalt Ansible de versleutelde back-upsleutels (sleutel A) op uit de version control. Ansible kan die sleutels met de eigen sleutel B ontsleutelen. Vervolgens geeft Ansible die ontsleutelde back-upsleutels (sleutels A) aan de database door, zodat de database de met sleutel A versleutelde back-up kan terugzetten.

Een beheerder kan met de storage key, sleutel B uit de secure storage halen. De beheerder kan vervolgens de versleutelde back-upsleutels (sleutel A) uit de version control halen en ze met sleutel B ontsleutelen. Vervolgens kan de beheerder de versleutelde back-up downloaden van Azure en met de ontsleutelde back-upsleutels (sleutel A) de back-up ontsleutelen.

CACI is ISO 27001 gecertificeerd en laat het beheer van Osiris regelmatig volgens ISAE auditen. De scope van de ISO 27001 dekt alle verwerkingen van persoonsgegevens binnen Osiris. De bijbehorende statement of applicability sluit geen relevante zaken uit. Het ISAE-rapport van 17 oktober 2024 meldt één beperking: "*Vastgesteld dat de uitgegeven toegangsrechten niet worden beoordeeld aan de hand van de autorisatiematrix".*[6]

1.9 Logging en monitoring

Voor logging kan onderscheid gemaakt worden tussen auditlogging en applicatielogging. Auditlogging ziet op de handelingen die binnen een applicatie worden verricht met betrekking tot de gegevens. De audit logging van Osiris is actief op elk database record. Per database record worden de volgende zaken bijgehouden:

- creatie gebruiker
- creatie datum
- creatie applicatie
- mutatie gebruiker
- mutatie datum
- mutatie applicatie

Van historietabellen (zie paragraaf 1.6) houdt Osiris de complete geschiedenis van wijzigingen bij.

Applicatielogging gaat om de correcte werking van de applicatie. In Osiris gebeurt dit op het niveau van systeemlogging. Standaardlogging bevat alleen het aanmelden en afmelden op een database. Bij een incident kan voor één sessie debuglogging met uitgebreidere logs aangezet worden door de ingelogde medewerker, zodat het mogelijk is om te controleren wat er misgaat. Na afloop van de sessie eindigt de debug logging automatisch.

CACI heeft in oktober 2024 een werkgroep logging opgestart met als doel om samen met de instellingen te komen tot een gewenste implementatie van logging. Ook SURF is vertegenwoordigd in de werkgroep. Vanuit de instellingen nemen onder andere functioneel beheerders en security officers deel aan de werkgroep.

CACI monitort de performance van de servers door bij te houden hoelang het duurt om elke request te beantwoorden. Als het beantwoorden van een request langer duurt dan een door CACI ingestelde norm, dan verzamelt het monitoringssysteem details over die request. Die details bevatten wel welke gebruiker de request gedaan heeft en welke pagina opgevraagd is,

[6] CACI: International Standard on Assurance Engagements Report (ISAE) 3402 Type II Voor de Osiris SaaS dienstverlening Periode: 1 juli 2023 tot en met 30 juni 2024, Ref: R2409-07; 17 oktober 2024

maar bevatten verder geen details uit de inhoud van die pagina. Daarnaast gebruikt CACI Endpoint Detection and Response (EDR) tooling om events op de virtuele servers te monitoren en de virtuele servers te scannen op mogelijke veiligheidsproblemen. Dit scannen gebeurt lokaal op de virtuele servers en eventuele problemen worden via een extern ingehuurd Security Operations Centre (SOC) gerapporteerd aan CACI. Deze scanning en monitoring heeft geen toegang tot persoonsgegevens van de gebruikers van Osiris.

1.10 Back-ups

Het doel van back-ups maken is het continu veiligstellen van de servers en databases van de applicatieomgevingen van het systeem, zodat in geval van een calamiteit recovery van gegevens kan worden uitgevoerd en/of servers kunnen worden hersteld. Hiertoe worden verschillende soorten back-ups gemaakt. De SaaS variant van Osiris kent drie typen back-ups[7]:

- Server back-up.
- Onsite database back-up (bij de housing en hostingpartij).
- Offsite database back-up (bij een subverwerker).

1.10.1 Server back-up

Interconnect maakt dagelijks een back-up van de virtuele servers die het voor CACI host. De bewaartermijn van deze back-ups is 7 dagen. Deze back-ups worden gebruikt om bij grote incidenten de virtuele servers te kunnen herstellen. Interconnect slaat deze back-ups op als onderdeel van hun aanbod voor virtuele servers. Deze back-ups kunnen incidenteel persoonsgegevens bevatten als Interconnect deze back-up maakt op precies het moment dat een student of een medewerker een bestand naar Osiris aan het uploaden is. In dat geval bevat de back-up het deel van het bestand dat de Student of de Medewerker al geüpload had. Daarbuiten bevatten deze back-ups geen persoonsgegevens.

1.10.2 Onsite database back-up

Oracle biedt bij hun Oracle Database Servers een optie aan om een ‘hot back-up’ te maken. Dit systeem volgt live alle veranderingen in de database en slaat al deze veranderingen incrementeel op. CACI gebruikt dit systeem om een ‘hot’ back-up van Osiris te maken. Deze back-up is versleuteld. CACI bewaart deze back-ups bij Interconnect. Voor de productieomgevingen worden deze back-ups 14 dagen bewaard. Dit betekent dat het over een periode tot 14 dagen terug, mogelijk is om van elk willekeurig moment gegevens onmiddellijk terug te zetten.

1.10.3 Offsite database back-up

De onsite back-ups worden dagelijks opgeslagen in een ‘immutable’ (niet wijzigbare) opslag in een Microsoft Azure omgeving. Doordat de opslag ‘immutable’ is, is een aanvaller, bijvoorbeeld in het geval van een ransomware aanval, niet in staat om back-ups van voor de aanval onleesbaar te maken.

Bij deze back-ups kan alleen de complete database teruggezet worden. CACI hanteert de volgende bewaartermijnen:

[7] CACI: Osiris Backup en Recovery; 16 april 2025

Tabel 4: bewaartermijnen offsite back-ups

Type back-up	Bewaartermijn
Dagelijks (incrementeel)	28 dagen
Wekelijks (volledig)	28 dagen
Maandelijks (volledig)	90 dagen
Kwartaal (volledig)	één jaar

Dit betekent dat het over een periode tot 28 dagen terug, mogelijk is om van elk willekeurig moment gegevens terug te zetten, met hoogstens enkele seconden dataverlies. Voor een periode van 90 dagen kan een maandelijkse back-up teruggezet worden.
Voor een periode van een jaar kan er een kwartaal back-up worden teruggezet.

Als er bij een calamiteit de onsite back-ups onleesbaar wordt en data uit de offsite back-up teruggezet wordt, is het gegevensverlies maximaal 24 uur.

Als bij een calamiteit zowel de onsite back-ups als de offsite back-ups onleesbaar worden, dan kan er teruggevallen worden op de back-ups van de virtuele machines en is het gegevensverlies maximaal 24 uur.

1.11 Verwijderen van gegevens

1.11.1 Verwijderen van gegevens uit database

De onderwijsinstelling kan uitgebreid, naar de eigen selectielijsten, bewaartermijnen vaststellen voor de verschillende gegevens. Na die bewaartermijn worden de tabellen opgeschoond. Osiris kent verschillende soorten van ‘verwijderen’:

- Het archiveren van een student: Docenten zien alleen actieve studenten. Door een student als ‘gearchiveerd’ te markeren, blijft de student nog in de database, maar wordt de student pas weer zichtbaar als de student weer op ‘actief’ is gezet.
- Het wissen van gegevens uit normale database tabellen: Als een rij of veld uit deze tabellen gewist wordt, verdwijnt deze ook direct uit de database.
- Het wissen van gegevens uit ‘historietabellen’: Als gegevens uit een van deze tabellen worden gewist, dan worden de gegevens verwijderd uit de basistabel, maar blijft het archief van wijzigingen bewaard in de bijbehorende historietabel.
- Het opschonen van de ‘historietabellen’: Als de basistabellen worden opgeschoond, dan worden ook de archieven van de verwijderde records verwijderd uit de bijbehorende historietabellen.

Indien de gegevens van een student integraal verwijderd worden, dan treedt een afwijkend mechanisme in werking:

- Van de records in een aantal tabellen wordt het studentnummer vervangen voor een nieuw nummer en worden alle direct identificerende gegevens gewist. Dit wordt gedaan bij de volgende tabellen:
    - Ten behoeve van analytics bij de tabellen: OST_H_STUDENT en OST_H_S_INSCHRIJFHIST

- Ten behoeve van Osiris Debiteur bij de tabellen OST_DEBITEUR_JOURNAALPOST, OST_OSIRIS_BANK_DETAILS, OST_BANK_OSIRIS_DETAILS, OST_AANMANING_SAMENGEVOEGD en OST_AANMANING_DETAILS.
- Ten behoeve van de financiële interface bij de tabellen OST_FINANCIEEL_FCODS en OST_FINANCIEEL_OSIDS

- Alle andere records van de student worden verwijderd, inclusief de historie in de historie tabellen.
- Alle andere aan de student gelinkte gegevens zoals documenten en mededelingen worden verwijderd.

1.11.2 Verwijderen gegevens bij einde dienstverlening

Bij het beëindigen van de dienstverlening maakt CACI na 90 dagen de accounts ontoegankelijk. Nog 90 dagen later verwijdert CACI de databases. Op dat moment verstuurt CACI aan de onderwijsinstelling een eerste notificatie van het vernietigen van data. De back-ups van de database worden volgens het back-up schema gewist. Dat betekent dat 1 jaar na het wissen van de database CACI ook de laatste back-up daarvan verwijdert. Op dat moment verstuurt CACI een tweede notificatie over het vernietigen van data.

1.12 Inzage in persoonsgegevens

Onderwijsinstellingen dienen hun eigen proces voor het afhandelen van inzageverzoeken en het faciliteren van de andere rechten van betrokkenen in te richten. In het kader van deze DPIA zijn drie inzageverzoeken ingediend bij TiU. TiU is immers verwerkingsverantwoordelijke (voor zowel de testomgeving als de productie-omgeving). De inzageverzoeken zijn via een webformulier naar de privacy officer gestuurd.

Op alle drie de verzoeken is een reactie gekomen. De reactie beperkte zich tot de gegevens die een gebruiker niet zelf in Osiris kan zien.

- Bij het inzageverzoek van de student, wees de privacy officer van TiU de student erop dat studenten in het studentportaal kunnen kijken, waar de student alles over zijn eigen inschrijving en voortgang en de basisgegevens kan inzien en gegevens kan corrigeren.
- In de tweede plaats heeft TiU enkele identifiers aangeleverd die de beheerder van Osiris bij een instelling wel kan zien, maar de student of medewerker zelf niet direct. Deze identifiers waren afkomstig uit de authenticatieserver van TiU en bevatten ook het laatste tijdstip van inloggen.
- In de derde plaats heeft TiU de betreffende identifiers en IP-adressen nog naar CACI doorgestuurd met de vraag wat zij extra konden vinden bij deze gegevens. CACI heeft in reactie hierop aangegeven dat zij bij geen van de inzageverzoeken van de medewerkers en studenten aanvullende gegevens over de betreffende persoon konden vinden.

De student kreeg de volgende informatie van de TiU (verkregen via CACI):

“CACI heeft in alle logfiles en auditfiles (in de acceptatieomgeving) gekeken welke data van de betreffende student zijn opgeslagen De volgende twee loggegevens zijn aanwezig:

Logbestanden **student** (2157188, [emailadres student] u659513)
In de database

- select * from stt_adf_log where melding like '%2157188% or melding like ‘%andsaat%' or melding like ‘u659513’;
    - 126836 - 2157188 - 16260 21-02-2025 14:05:01
    - 126836 - 2157188 - 16260 - INSERT 21-02-2025 14:05:02

Toelichting: Dit wordt weggeschreven voor debug doeleinden. Dit kan worden aangezet, en dus ook uitgezet, door TiU zelf via de config IO/LOG-AANMELDPROCES).

Op de applicatieserver:

- Grep op: u659513
  grep -i u659513 /xxxxxx/*TIUACC/logs/

  /xxxxxx/*-TIUACC/logs/access.log02440:2025-03-14 10:43:03 GET d1e64240-ee2c-4030-a303-6ee5377b33fc-00007b8c 0 /osiris_docent/[pad]/Bewijs%20University%20of%20Nigeria%20-%20[NAAM]%20[NAAM]%20u659513.docx?docid=1362614&dcf=1gjvtpgco_1 200 15348
  /xxxxxx/*-TIUACC/logs/access.log02440:2025-03-14 10:43:08 GET d1e64240-ee2c-4030-a303-6ee5377b33fc-00007b90 0 /osiris_docent/downloaddocument/Diploma%20University%20of%20Nigeria%20-%20[NAAM]%20[NAAM]%20u659513.docx?docid=1362615&dcf=1gjvtpgco_1 200 15348

Toelichting: deze download wordt door standaardcomponenten van het framework afgehandeld en hierbij wordt deze log weggeschreven.”

1.13 Mobiele App (Studenten)

CACI biedt, naast de webinterface voor studenten, ook een app voor mobiele telefoons aan. Deze is zowel beschikbaar voor iOS als voor Android. De mobiele app is gemaakt met hetzelfde framework waarmee ook de webinterface gemaakt is, en biedt ook dezelfde functionaliteiten.

Boven op de functionaliteiten van de webinterface, biedt de mobiele app aan de onderwijsinstellingen ook de mogelijkheid om pushberichten naar de student(en) te sturen. De inhoud van deze berichten kan door de onderwijsinstelling zelf geconfigureerd worden. Om de pushberichten te versturen maakt de app op iOS gebruik van Apple Push Notifications (APN) en op Android van Firebase Google Cloud Push. Beiden vereisen dat de telefoon zich aanmeldt met een API-key, dat de app zich aanmeldt met een ID en dat de app die ID met Osiris deelt zodat de pushberichtendienst de berichten correct kan doorsturen. De berichten van de onderwijsinstelling worden in platte tekst met de pushberichten meegestuurd. Doordat TiU geen gebruik maakt van de pushberichten, is dit niet verder getest voor deze DPIA.

1.14 Contractstructuur

De onderwijsinstellingen hebben ieder een individueel contract met CACI B.V. voor het afnemen van Osiris.[8] Naast het leveringscontract hebben de instellingen een verwerkersovereenkomst[9] met CACI afgesloten. Deze DPIA gaat ervan uit dat de standaard SURF Model Verwerkersovereenkomst versie 3.0 of 4.0 wordt gebruikt. Als gevolg hiervan worden niet alle clausules van de verwerkersovereenkomst van TiU beoordeeld. De specifieke clausule over de locatie van de gegevensverwerking uit de verwerkersovereenkomst van TiU is wel meegenomen (zie hoofdstuk 7), omdat het goed mogelijk is dat andere instellingen dezelfde clausule hanteren. Ook de bijlagen van de verwerkersovereenkomst van TiU wordt als referentie gebruikt.

CACI heeft een (sub)verwerkersovereenkomst gesloten met Interconnect en met EnableU.

Voor de back-ups in de Microsoft Azure cloud geldt de standaard verwerkersovereenkomst van Microsoft (Products and Services Licensing Agreement).[10]

[8] In het geval van TiU was er een oorspronkelijk contract met CapGemini als leverancier. CACI heeft de applicatie en contracten in 2016 van CapGemini overgenomen.

[9] In principe werken ho-instellingen met het SURF-template. Het mbo hanteert het template vanuit het privacy convenant. Soms wordt een Arbit-model gebruikt vanuit aanbestedingen.

[10] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA, geraadpleegd op 7 augustus 2025.

2 Betrokkenen en persoonsgegevens

Bij het onderzoeken van de privacyrisico's van een gegevensverwerking is het belangrijk om te bekijken welke typen gegevens van welke groepen betrokkenen worden verwerkt. Dit hoofdstuk geeft een overzicht van alle typen gegevens van de verschillende groepen betrokkenen.

Dit hoofdstuk is geschreven over de gegevensverwerkingen zoals die bij TiU zijn aangetroffen. Andere onderwijsinstellingen kunnen bij het inrichten van Osiris ervoor kiezen om andere gegevens te verwerken en/of om andere processen in te richten in Osiris. Daarom moeten onderwijsinstellingen die Osiris inzetten hun eigen inventarisatie van de verwerkte persoonsgegevens maken. Deze inventarisatie dient daarbij ter referentie.

2.1 Categorieën van betrokkenen

Bij het gebruik van Osiris door onderwijsinstellingen worden de volgende categorieën betrokkenen onderscheiden:

Tabel 5: Overzicht mogelijke betrokkenen

Groep	Configuratie TiU
Studenten	Studenten zijn bij TiU ingedeeld op basis van de status van hun inschrijving. TiU kent negen verschillende factoren in deze status, zoals aangemeld, gegevens compleet, betaling collegegeld compleet, etc. Afhankelijk van deze status, hebben de studenten meer of minder mogelijkheden binnen Osiris. Door middel van deze statussen maakt Osiris ook het onderscheid tussen aspirant-studenten, actieve studenten, contractstudenten en alumni.
Medewerkers	TiU heeft 64 verschillende medewerkersrollen ingeregeld. Daar bovenop heeft TiU nog 12 taken gedefinieerd die boven op een rol kunnen komen. Afhankelijk van de rol en taken hebben de medewerkers verschillende toegang tot gegevens en verschillende rechten om gegevens aan te passen of om processtappen uit te voeren. TiU onderscheidt de volgende medewerkersrollen: Registration Officer Diplomeerder Resultaatverwerker Medewerker Student Desk Studentmedewerker Student Desk Procesondersteuner digitaal toetsen Roosteraar voorzieningen Tentamenondersteuner

	Immigration Coordinator Medewerker Language Center Scholarship Coordinator International Admissions Coordinator Bachelor International Admissions Coordinator (Pre) Master Admissions Coordinator Research Master Admissions Coordinator Numerus Fixus Postmaster Coordinator International Admissions Diploma Evaluator International Admissions Officer International Admissions Assistant Studentenpsycholoog Assistent Studentenpsycholoog Debiteuren beheerder Administrateur Finance & Control Immigration Assistant Secretaris Examencommissie Ondersteuner examencommissie (Ondersteuner) Studentendecaan Onderwijscoordinator Onderwijscoordinator TLS Onderwijscoordinator TISEM Toelatingscoordinator BSA coordinator Studentmedewerker Begeleider LC Behandelaar Matching Beoordelaar Matching Beoordelaar Admissions (Pre) Master Beoordelaar Toelating (Pre) Master Beoordelaar Admissions Research Master Housing Officer Beleidsmedewerker Medewerker Exchange Assistent Exchange In(&Ex)terne Accountant F&C - medewerker FSC Medewerker Evaluaties Stagebegeleider Medewerker Bibliotheek Medewerker Marketing & Communicatie Medewerker Secretariaat EST Academic Director Scriptiebegeleider Docent Toetsdeskundige Program Activity Coordinator Coördinator Wiskunde Testimonium

	PhD Coordinator Developer Datawarehouse (IRAP) Nationaal Toelatings Coordinator (Pre) Master Beoordelaar Toelating Postmaster Accountancy Administratief Ondersteuner Maatschappelijkwerker Optimaliseur Bekostigingen Mentor
Beheerders TiU	De beheerders van TiU hebben binnen Osiris ook accounts. Via deze accounts zijn onder andere de rechten aan te passen.

2.2 Categorieën van persoonsgegevens

Het begrip persoonsgegeven is breed en behelst allerlei soorten gegevens over een persoon.

> *"persoonsgegeven": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4, lid 1 AVG).*

2.2.1 Studenten

Van studenten worden verschillende categorieën persoonsgegevens verwerkt. Zo wordt onder meer informatie verwerkt ten behoeve van de inschrijving, de opleiding en de studiebegeleiding. De onderstaande tabellen geven weer welke persoonsgegevens over de studenten Privacy Company tijdens het testen bij TiU aangetroffen heeft. De gegevensverwerkingen zijn naar verschillende tabellen uitgesplitst om op die manier gegevensverwerkingen die per instelling anders kunnen zijn uit elkaar te houden. Ook lopen sommige gegevensverwerkingen via andere functionele of technische modules, bijvoorbeeld via ‘Zaak’.

De tabel geeft weer of de persoonsgegevens bijzondere persoonsgegevens zijn, strafrechtelijke persoonsgegevens, of het nationale identificatienummer betreft en of anderszins gevoelige persoonsgegevens betreft. Paragraaf 2.3 t/m 2.6 lichten deze beoordelingen toe.

De gegevens over studenten die tijdens het reguliere inschrijvingsproces worden verwerkt, zijn weergegeven in Tabel 6: Inschrijvingsgegevens van studenten die via Studielink inschrijven. De Technische Appendix geeft verdere details op veldniveau weer van de gegevens die via studielink uitgewisseld worden.

Tabel 6: Inschrijvingsgegevens van studenten die via Studielink inschrijven

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	BSN	Gevoelig (anders)	Bronnen

Studielink ID + SIS IDs + samengestelde naam					Studielink
Volledige naam					Studielink
BSN of anders onderwijsnummer			√		Studielink
Adresgegevens				Soms (zie ‘geheim adres’)	Studielink
Geheim adres (ja/nee)				√	Studielink
Contactgegevens					Studielink
Correspondentietaal					Studielink
Demografische gegevens (Geslacht, Geboortedatum, Geboorteplaats)					Studielink
Vestigingsinformatie					Studielink
Nationaliteit					Studielink
Verblijfsstatus					Studielink
Ooit ingelogd met DigID (ja/nee)					Studielink
Persoonsverificatie					Onderwijs-instelling
Datum en status aanmelding					Studielink
Gegevens opleiding					Studielink
Rangnummer					Onderwijs-instelling
Gegevens betaling				√	Studielink Onderwijs-instelling
Vragen, antwoorden en mededelingen					Studielink

					Onderwijs-instelling
Deelname studiekeuzecheck					Studielink
Gegevens vooropleiding					Studielink
Datum afmelding bij studielink					Studielink
Restitutie collegegeld (ja/nee)					Onderwijs-instelling
Herinschrijving					Studielink
Wijziging inschrijving					Studielink
Overlijden student[11]					Studielink Onderwijs-instelling
Datum selectie					Onderwijs-instelling
Pasfoto Student					Student

Sommige studenten, bijvoorbeeld contactstudenten, schrijven buiten Studielink om, direct bij de instelling in. Tabel 7: Inschrijvingsgegevens van studenten die direct bij TiU inschrijven, geeft weer welke gegevens van deze studenten verwerkt worden:

Tabel 7: Inschrijvingsgegevens van studenten die direct bij TiU inschrijven

Categorie persoonsgegevens	**Bijzonder**	**Straf-rechtelijk**	**BSN**	**Gevoelig (anders)**	**Bronnen**
SIS IDs + samengestelde naam					Student
Volledige naam					Student
BSN of anders onderwijsnummer			√		Student

[11] Het overlijdensbericht van de student bevat de naam van de medewerker die het bericht ingevoerd heeft. Indien de student overleden is, zijn de gegevens over de student geen persoonsgegevens volgens de AVG. Wel is nog het (medische) beroepsgeheim van toepassing op deze gegevens.

Adresgegevens				Soms (zie ‘geheim adres’)	Student
Geheim adres (ja/nee)				√	Student
Contactgegevens					Student
Correspondentietaal					Student
Demografische gegevens (Geslacht, Geboortedatum, Geboorteplaats)					Student
Vestigingsinformatie					Student
Nationaliteit					Student
Verblijfsstatus					Student
Persoonsverificatie					Onderwijs-instelling
Datum en status aanmelding					Onderwijs-instelling
Gegevens opleiding					Student
Gegevens betaling				√	Onderwijs-instelling
Gegevens vooropleiding					Onderwijs-instelling
Restitutie collegegeld (ja/nee)					Onderwijs-instelling
Herinschrijving					Onderwijs-instelling
Wijziging inschrijving					Onderwijs-instelling
Overlijden student					Onderwijs-instelling
Pasfoto student					Student

Indien een student geen verblijfsstatus heeft in Nederland, kan de student via TiU een verblijfsvergunning aanvragen. De gegevens die TiU verwerkt voor deze aanvraag zijn weergegeven in Tabel 8: Gegevens aanvraag verblijfsvergunning student. In de Technische Appendix staan details op veldniveau weergegeven.

Tabel 8: Gegevens aanvraag verblijfsvergunning student

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	Nat. ID nummer	Gevoelig (anders)	Bronnen
Nederlands Registratie nummer/ uniek ID-nummer			√		IND
Gegevens identificerend document			√		Student
Kopie identificerend document			√		Student
Aanvraag gegevens verblijfsdocument				√	Student
Status en resultaat aanvraag				√	IND
Gegevens verstrekte verblijfsvergunning	√[12]			√	IND
Huwelijk of geregistreerd partnerschap.					Student

Na inschrijving voor een opleiding, kan een student zich inschrijven voor cursussen, toetsen, minors en specialisaties. De gevolgde vakken leveren studieresultaten/ beoordeling op en op basis daarvan wordt in sommige gevallen een bindend studieadvies gegeven. De gegevens die TiU daarbij verwerkt, zijn weergegeven in: Tabel 9: Gegevens bij inschrijving, beoordeling en studieadvies.

Tabel 9: Gegevens bij inschrijving, beoordeling en studieadvies

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	Nat. ID nummer	Gevoelig (anders)	Bronnen
Gegevens inschrijving					Student
Studieresultaten				√	Docent

[12] Bevat gegevens over het afnemen van een TBC-onderzoek.

Bindend studieadvies				√	Onderwijs-instelling

Osiris heeft een module voor de begeleiding van studenten. Bij TiU is die zo ingericht dat de onderwijscoördinator daar notities aan toe kan voegen. Verder heeft TiU in Osiris verschillende processen ingericht voor het aanvragen van voorzieningen, bijvoorbeeld als de student een handicap heeft. Ook heeft TiU een proces ingericht voor het opleggen van sancties aan studenten. Daarnaast kan de student aanvragen doen voor de uitreiking van het bachelordiploma, vrijstellingen of een gesprek met de studentenpsycholoog. Ook kan de student bij TiU via Osiris in beroep gaan, bezwaar aantekenen en klachten indienen. De gegevens die daarbij verwerkt worden, staan vermeld in Tabel 10: Begeleiding, voorzieningen, aanvragen en zaken

Tabel 10: Begeleiding, voorzieningen, aanvragen en zaken

Categorie persoonsgegevens	**Bijzonder**	**Straf-rechtelijk**	**Nat. ID nummer**	**Gevoelig (anders)**	**Bronnen**
Categorie begeleidings-notitie	Mogelijk			√	Onderwijs-coördinator
Inhoud begeleidings-notitie (vrije tekst)	Mogelijk	Mogelijk		Mogelijk	Onderwijs-coördinator
Toegekende voorziening	Mogelijk			√	Decaan
Toelichting voorziening	Mogelijk			√	Decaan
Aanmelden uitreiking bachelordiploma					Student
Aanvragen studentenpsycholoog				√	Student
Indienen beroep				√	Student
Indienen bezwaar				√	Student
Indienen klacht	Mogelijk			√	Student
Verzoek om vrijstelling					Student
Begeleidende documenten vrijstelling	Mogelijk			Mogelijk	Student
Opgelegde sanctie		Mogelijk		√	Onderwijs-instelling

TiU gebruikt Osiris ook om de bezoeken aan de studentenpsycholoog aan te vragen en voor de studentenpsychologen om de bezoeken te registreren en de verslagen van de gesprekken vast te leggen. De persoonsgegevens van studenten die daarbij verwerkt worden, staan in: Tabel 11: Persoonsgegevens bezoek studentenpsycholoog.

Tabel 11: Persoonsgegevens bezoek studentenpsycholoog

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	Nat. ID nummer	Gevoelig (anders)	Bronnen
Registratie bezoeken				√	
Verslaglegging bezoeken	√			√	

Tenslotte verwerkt Osiris ook nog een aantal technische gegevens. Deze gegevens zijn noodzakelijk voor het correct functioneren van Osiris. Deze gegevens zijn weergegeven in Tabel 12: Technische gegevens

Tabel 12: Technische gegevens studenten

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	Nat. ID nummer	Gevoelig (anders)	Bronnen
IP-adres					Osiris
Inloggegevens					Instelling
Auditlog				√	Osiris

2.2.2 Medewerkers onderwijsinstellingen

Van medewerkers van de onderwijsinstellingen kunnen bij het gebruik van Osiris de volgende gegevens worden verwerkt:

Tabel 13: Categorieën persoonsgegevens medewerkers

Categorie persoonsgegevens	Bijzonder	Strafrechtelijk	BSN	Gevoelig (anders)	Bronnen
Basisgegevens					
Registratienummer					Instelling
Naam					Medewerker
Geslacht					Medewerker
Contactgegevens					Medewerker
E-mailadres (intern)					Medewerker

Opleidingsgegevens					
Vakken					Instelling
Rooster					Instelling
Studenten				√	Instelling
Resultaten van studenten					Instelling
Docentnotities				√	Instelling
Gegevens rond begeleiding van studenten					
Gespreksverslagen decanen of studiebegeleiders				√	Instelling
Technische en gebruiksgegevens					
IP-adres					Osiris
Inloggegevens					Instelling
Auditlogs				√	Osiris

2.2.3 Beheerders onderwijsinstelling

De beheerdersaccounts van TiU hebben uitgebreidere rechten dan gewone medewerkers. Een aantal van de acties waar de beheerders rechten toe hebben, kunnen uitgebreidere (audit) logging triggeren dan bij andere medewerkers. Daardoor kan Osiris over de beheerders ook meer persoonsgegevens genereren:

Tabel 14: Technische gegevens medewerkers

Categorie persoonsgegevens	Bijzonder	Straf-rechtelijk	Nat. ID nummer	Gevoelig (anders)	Bronnen
IP-adres					Osiris
Inloggegevens					Instelling
Auditlog				√	Osiris

2.3 Bijzondere persoonsgegevens

De AVG verbiedt in beginsel de verwerking van bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag

of seksuele gerichtheid (artikel 9 lid 1 AVG). Op dit verwerkingsverbod gelden de verschillende uitzonderingen die beschreven staan in artikel 9, lid 2 AVG en in de Uitvoeringswet AVG (UAVG). In Osiris zitten geen standaardvelden voor bijzondere persoonsgegevens en het is niet ingericht om bijvoorbeeld als patiëntendossier te worden gebruikt. Vanwege de reguliere doeleinden waar Osiris voor bestemd is kunnen wel bijzondere persoonsgegevens verwerkt worden.
De kopie van het identificerend document is bedoeld ter verificatie van de identiteit, niet voor unieke identificatie met behulp van biometrie. In deze context geldt dit dus niet als bijzonder persoonsgegeven.

Tabel 15: Aangetroffen bijzondere persoonsgegevens

Persoonsgegeven	Toelichting
Gegevens verstrekte verblijfsvergunning	Bevat of een TBC test is afgenomen
Categorieën begeleidingsnotitie van de onderwijs coördinator	Bij TiU heeft de hoofdcategorie 'persoonlijk' de volgende subcategorieën: Suborderwerp / Omschrijving AD(HD) / AD(HD) ASS / ASS BLESSURE / Blessure / ongeval BO STATUS / BO Status CHRON ZIEKTE / Chronische ziekte CORONA / Corona CULT PROBL / Culturele problemen DYSLEXIE / Dyslexie FAM OMST / Familie omstandigheden FUNCTIE / Functiebeperking GENDER / Gender problematiek HOUSING / Huisvesting MANTELZORG / Mantelzorg PSY PROBL / Psychische problemen VERSLAVING / Verslaving ZIEKTE / Ziekte ZWANGER / Zwanger Een aantal ervan zijn direct medische of psychische diagnoses.
Inhoud begeleidingsnotitie van de onderwijs coördinator (vrije tekst)	Dit veld kan, doordat het vrije tekst is, bijzondere persoonsgegevens bevatten. Gezien de aard van notities en de mogelijke categorieën is de kans hierop reëel.
Toegekende voorzieningen	Bij TiU zijn de meeste voorzieningen aanwijzingen zonder dat er een aandoening benoemd wordt, maar een aantal voorzieningen bevatten deze wel: - Gebruik telefoon/meetapparatuur/medicatie m.b.t. diabetes - Student heeft epilepsie - Bij migraineaanval breekt student tentamen af en verlaat de zaal
Toelichting voorziening	Dit veld kan, doordat het vrije tekst is, bijzondere persoonsgegevens bevatten. Gezien de aard van notities en de mogelijke categorieën, is de kans hierop reëel.

Indienen klacht	Afhankelijk van de klacht, kunnen bij het indienen ervan bijzondere persoonsgegevens opgenomen worden in vrije tekstvelden of begeleidende documenten.
Begeleidende documenten vrijstelling	Deze documenten kunnen bijzondere persoonsgegevens bevatten.
Verslaglegging bezoeken studentenpsycholoog	Deze bevatten informatie over de (psychische) gezondheid van de student.

Er zijn geen verwerkingen aangetroffen waarbij bijzondere persoonsgegevens van medewerkers worden verwerkt in Osiris.

2.4 Strafrechtelijke gegevens

Persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen zijn volgens artikel 10 AVG strafrechtelijke persoonsgegevens.

Tabel 16: Aangetroffen strafrechtelijke gegevens

Persoonsgegeven	Toelichting
Inhoud begeleidingsnotitie van de onderwijs coördinator (vrije tekst)	Dit veld kan, doordat het vrije tekst is, strafrechtelijke gegevens bevatten. Gezien de aard van notities, is de kans, hoewel klein, wel aanwezig. Een situatie waarin dit bijvoorbeeld kan voorkomen is als een student door een eerdere veroordeling geen VOG kan krijgen voor een stageplaats.
Opgelegde sanctie	Dit betreft disciplinaire sancties opgelegd door TiU. Het kan voorkomen dat een incident zowel via een sanctie als via het strafrecht afgehandeld wordt. In deze gevallen kan de sanctie ook verwijzen naar de strafrechtelijke procedure. Ook is het mogelijk dat de sanctie een concrete beschrijving van strafbare feiten bevat, mogelijkerwijs kwalificeert dit als een bewezenverklaring en daarmee als strafrechtelijke gegevens.[13]

Onderwijsinstellingen zijn ook verplicht om een meldcode huiselijk geweld op te stellen.[14] Het verwerken van strafrechtelijke gegevens kan onderdeel zijn van de meldcode.

2.5 Nationale identificatienummers

Onderwijsinstellingen verwerken nationale identificatienummers in Osiris. Iedereen die onderwijs volgt dat door de overheid wordt bekostigd, heeft te maken met het persoonsgebonden nummer (PGN) (artikel 1.1 onder w WHW). Onderwijsinstellingen zijn

[13] Zie: ECLI:NL:HR:2009:BH4720, voorheen LJN BH4720, Hoge Raad, 08/00898, laatst geraadpleegd op 22 juni 2025

[14] https://www.rijksoverheid.nl/onderwerpen/huiselijk-geweld/meldcode, geraadpleegd op 9 oktober 2025

verplicht het PGN te gebruiken in hun administratie (artikel 7.31 e WHW).[15] Het PGN is het BSN, zoals bedoeld in artikel 1, sub b Wet algemene bepalingen burgerservicenummer (Wabb), of indien een student geen BSN kan verstrekken, het onderwijsnummer als bedoeld in artikel 7.31 e lid 3 WHW.

De gegevensuitwisseling in het kader van Erasmus Without Paper (EWP), bevat het nationale identificatienummer horend bij de nationaliteit van de student. Osiris gebruikt hierbij een 'European Student Identifier' die door Osiris zelf gegenereerd wordt. Het datamodel van EWP specificeert echter het 'nationale identificatienummer' niet verder. Het is daardoor mogelijk dat buitenlandse onderwijsinstellingen wel hun nationale identificatienummer meesturen.

Tabel 17: Aangetroffen nationale identificatienummers

Persoonsgegeven	Toelichting
BSN	Verplicht bij door de overheid bekostigd onderwijs.
Nederlands Registratie nummer/ uniek ID-nummer	Dit nummer wordt door de Nederlandse overheid uitgegeven aan elke persoon die een verblijfsvergunning voor Nederland aanvraagt.
Gegevens identificerend document	Dit bevat het nationale identificatienummer dat vermeld is op het identificerende document.
Kopie identificerend document	Dit bevat het nationale identificatienummer dat vermeld is op het identificerende document.
Nationale identificatienummer voor Erasmus Without Paper	Mogelijkerwijs bevat dit het nationale identificatienummer van buitenlandse studenten die naar Nederland komen.

2.6 Overige gevoelige gegevens

Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog risico met zich meebrengen.[16] Gevoelige persoonsgegevens zijn onder meer gegevens over de financiële situatie van betrokkenen en gegevens die betrekking hebben op kwetsbare groepen.

De Autoriteit Persoonsgegevens verwoordt dit als volgt:

"Er zijn ook gegevens die niet expliciet in de AVG zijn benoemd als gevoelig, maar die wel een grotere impact hebben op iemands privacy dan gewone persoonsgegevens. Dit noemen we gevoelige persoonsgegevens.

Persoonsgegevens die over het algemeen als privacygevoelig worden beschouwd, zijn:

- *gegevens over elektronische communicatie;*
- *locatiegegevens;*
- *financiële gegevens (zoals inkomen of koopgedrag);*

[15] https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs, geraadpleegd op 18 oktober 2022.

[16] Model DPIA Rijksdienst, versie 2.0.

- *het burgerservicenummer (BSN).”*[17]

In de configuratie van TiU heeft Privacy Company de volgende gevoelige persoonsgegevens aangetroffen:

Tabel 18: Aangetroffen gevoelige persoonsgegevens

Persoonsgegeven	**Toelichting**
Adresgegevens indien het een geheim adres betreft	Studielink geeft door of het adres van een student een geheim adres betreft. Dit gebeurt bijvoorbeeld indien de student bedreigd wordt.
Gegevens betaling	Dit betreft zowel wie er voor de student betaalt als de betaalwijze en of het een gespreide betaling betreft.
Aanvraag gegevens verblijfsdocument	Deze bevatten onder andere gegevens over de ouders van de student, huwelijkse staat, diens reisplannen, nationaliteit, gegevens over het financiële vermogen en de betaling van de aanvraag.
Status en resultaat aanvraag verblijfsdocument	Deze bevatten onder andere een codering waarom de aanvraag afgewezen is.
Gegevens verstrekte verblijfsvergunning	Deze bevatten onder andere een uniek toegekend ID-nummer, antecedenten en betalingsgegevens.
Studieresultaten	Inherent gevoelige gegevens
Bindend studieadvies	Inherent gevoelige gegevens

[17] Autoriteit Persoonsgegevens: Wat zijn persoonsgegevens? URL: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#gevoelige-persoonsgegevens (laatst bezocht op 2 juni 2025)

<table>
<tr><td>Categorie begeleidingsnotitie</td><td>Bij de TiU heeft de hoofdcategorie ‘persoonlijk’ de volgende subcategorieën:<table><tr><th>Subonderwerp</th><th>Omschrijving</th></tr><tr><td>AD(HD)</td><td>AD(HD)</td></tr><tr><td>ASS</td><td>ASS</td></tr><tr><td>BLESSURE</td><td>Blessure / ongeval</td></tr><tr><td>BO STATUS</td><td>BO Status</td></tr><tr><td>CHRON ZIEKTE</td><td>Chronische ziekte</td></tr><tr><td>CORONA</td><td>Corona</td></tr><tr><td>CULT PROBL</td><td>Culturele problemen</td></tr><tr><td>DYSLEXIE</td><td>Dyslexie</td></tr><tr><td>FAM OMST</td><td>Familie omstandigheden</td></tr><tr><td>FUNCTIE</td><td>Functiebeperking</td></tr><tr><td>GENDER</td><td>Gender problematiek</td></tr><tr><td>HOUSING</td><td>Huisvesting</td></tr><tr><td>MANTELZORG</td><td>Mantelzorg</td></tr><tr><td>PSY PROBL</td><td>Psychische problemen</td></tr><tr><td>VERSLAVING</td><td>Verslaving</td></tr><tr><td>ZIEKTE</td><td>Ziekte</td></tr><tr><td>ZWANGER</td><td>Zwanger</td></tr></table></td></tr>
<tr><td>Inhoud begeleidings-notitie (vrije tekst)</td><td>Zie: ‘Categorie Begeleidingsnoties’</td></tr>
<tr><td>Toegekende voorziening</td><td>Dit betreft voorzieningen voor handicaps die het leren van de student bemoeilijken.</td></tr>
<tr><td>Toelichting voorziening</td><td>Dit betreft voorzieningen voor handicaps die het leren van de student bemoeilijken.</td></tr>
<tr><td>Aanvragen studentenpsycholoog</td><td>Dit betreft zowel het feit dat er een gesprek aangevraagd is als de inhoud van de aanvraag.</td></tr>
<tr><td>Indienen beroep</td><td>Dit betreft zowel het feit dat een beroep is ingediend als de inhoud van het beroep.</td></tr>
<tr><td>Indienen bezwaar</td><td>Dit betreft zowel het feit dat er een bezwaar is ingediend als de inhoud van het bezwaar.</td></tr>
<tr><td>Indienen klacht</td><td>Dit betreft zowel het feit dat een klacht is ingediend als de inhoud van de klacht.</td></tr>
<tr><td>Begeleidende documenten vrijstelling</td><td>Deze kunnen informatie over de persoonlijke omstandigheden van de student bevatten.</td></tr>
<tr><td>Opgelegde sanctie</td><td>Dit betreft zowel het feit dat er een sanctie is opgelegd als de inhoud van de sanctie.</td></tr>
</table>

Registratie bezoeken studentenpsycholoog	Dit betreft het feit dat er een bezoek aan de studentenpsycholoog is geweest.
Verslaglegging bezoeken studentenpsycholoog	Dit betreft zowel het feit dat er een bezoek aan de studentenpsycholoog is geweest, als de inhoud van de verslaglegging.

Daarnaast kunnen instellingen onder bepaalde voorwaardenvoorwaarden financiële ondersteuning bieden aan studenten wegens bijzondere omstandigheden (artikel 7.51 WHW). Instellingen kunnen dit administreren in Osiris. TiU heeft hier echter een apart proces voor.

2.6.1 Notities

In de inrichting van TiU kunnen de decaan en de studentenpsychologen notities maken bij de student. Doordat dit een vrij tekstveld is, kunnen deze notities ook gevoelige gegevens bevatten.

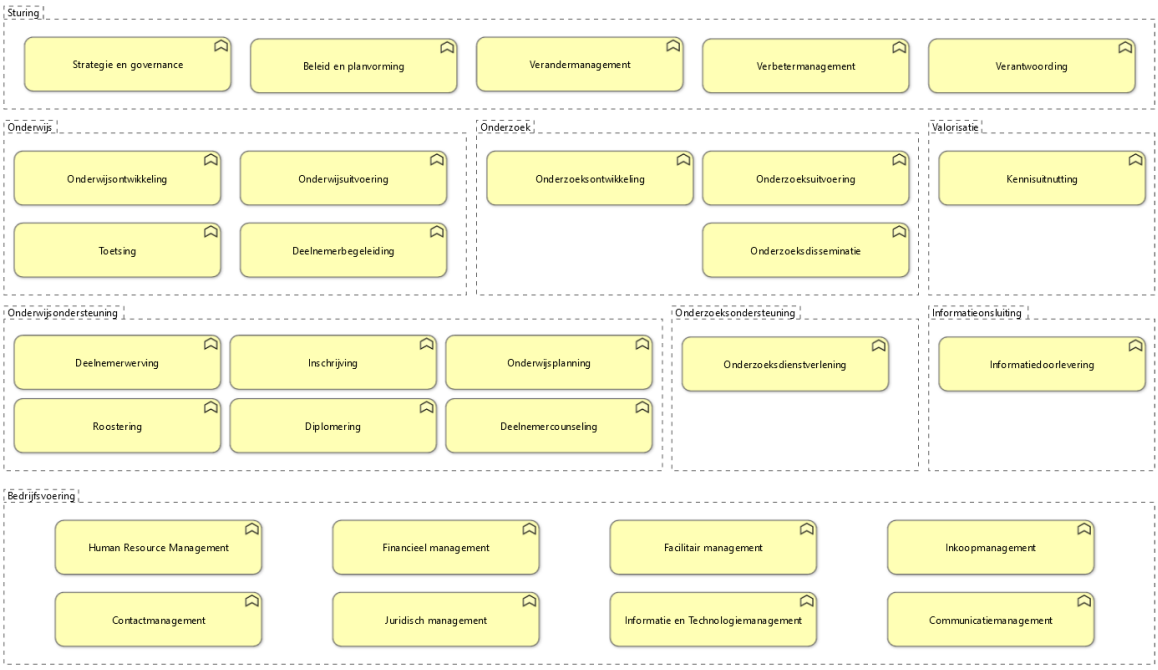
2.6.2 Geüploade documenten

Bij verschillende processen in Osiris, vooral in de module ‘zaak’ kunnen de studenten of de medewerkers documenten uploaden. Dat kan bijvoorbeeld gaan om een onderbouwing bij het verzoek om een vrijstelling aan de examencommissie, maar ook bijvoorbeeld bij het aanvragen van een verblijfsvergunning of een voorziening moet de student diverse documenten uploaden. Deze documenten kunnen gevoelige inhoud hebben. In sommige gevallen kan ook de bestandsnaam zelf al gevoelige informatie onthullen.

3 Verwerkingen

Om de rechtmatigheid van gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om de gegevensverwerkingen die binnen de scope van deze DPIA vallen in kaart te brengen. De hogescholen gebruiken Osiris voor uiteenlopende doelen en op verschillende manieren. De doelen staan beschreven in het volgende hoofdstuk. De samenwerkende Nederlandse instellingen voor Hoger Onderwijs hebben een standaardoverzicht gemaakt van de verwerkingen die zij moeten uitvoeren in het HORA model.[18]

Figuur 2: HORA Bedrijfsfunctiemodel op hoofdlijnen



Osiris kan niet voor al deze activiteiten worden gebruikt. Het is vooral gericht op het verwerken van gegevens van studenten, en is dan ook in gebruik voor de domeinen Onderwijs, Onderzoek en Onderwijsondersteuning.

3.1 Verwerkingen van gegevens van studenten

In onderstaande tabel is een overzicht gegeven van de typen verwerkingen waarin HORA voorziet met betrekking tot studentgegevens.

Tabel 19: Verwerkingsactiviteiten studenten volgens HORA

Verwerkingsactiviteiten studenten volgens HORA		
Onderzoeksregistratie	Studieinschrijving	Deelnemerinschrijving

[18] URL: https://hora.surf.nl/index.php/Bedrijfsfunctiemodel, geraadpleegd op 8 februari 2023.

Studiekeuzebegeleiding	Identiteitgegevensbeheer	Lesroosterconstructie
Bibliotheekgegevensbeheer	Autorisatiegegevensbeheer	Roosterpublicatie
Toetsbeoordeling	Learning management	Bindend studieadvies
Toetsroosterconstructie	Onderwijsuitvoeringsevaluatie	Persoonlijke situatiebegeleiding
Arbeidsmarktbegeleiding	Stagebegeleiding	Basisgegevensbeheer hoger onderwijs
Waardedocumentverstrekking	Aanmeldingsregistratie	Studieloopbaanbegeleiding
Vraagprognotisering	Toetsvoorbereidingsfunctie	Toetsuitvoering
Betalingsgegevensbeheer	Onderwijsactiviteitenplanning	Toepassing leermaterialen
Deelnemermatching	Stageplaatsmatchingfunctie	Voorbereiding onderwijsuitvoering
Roosterwijziging	Lesgroepvorming	Auteurgegevensbeheer
Kwalificatiecontrole	Voortgangsbewaking	Auteuridentificatie
Inzet- en middelenplanning	Afhandeling bezwaren en beroepen	Deelnemeruitschrijving
Deelnemer herinschrijving	Onderwijsuitvoeringsbegeleiding	Factuurgegevensbeheer
Relatiegegevensbeheer	Roosterconstructiefunctie	Digitaal portfolio
Debiteurgegevensbeheer	Stagetrajectgegevensbeheer	

Niet alle instellingen gebruiken Osiris voor al deze verwerkingen. Ook is het mogelijk dat instellingen Osiris voor nog andere verwerkingen gebruiken, die niet in bovenstaande tabel staan.

Tabel 20: Aanvullende mogelijke verwerkingsactiviteiten gegevens studenten in Osiris

Aanvullende verwerkingsactiviteiten gegevens studenten in Osiris		
Registratie en analyse gebruik app	Verslagen van begeleiding door het decanaat	Verslaglegging psychologische ondersteuning

Lijst studentenvergunning via International Office	Registratie van agressie en geweld	Beschikbaar stellen van een gewaarmerkte kopie van het diploma
Logging gebruiksgegevens	Analyse van studiegegevens	Analyse van agressie- en geweldsincidenten
Verwerkingen met betrekking tot fraudebestrijding	Registratie calamiteiteninformatie	Archivering en verwijdering
Verifiëren studentenstatus voor beschikbaar stellen van woningruimte	Testen Osiris (indien met productiegegevens)	Meewerken aan opsporingsverzoeken
Support gebruik Osiris	Het omzetten van de persoonsgegevens in de database naar een syntetische gegevensset ten behoeve van testen	

3.2 Verwerkingen van gegevens van medewerkers

De onderwijsinstellingen verwerken in Osiris ook gegevens van medewerkers. Het gaat om de volgende verwerkingen:

Tabel 21: Verwerkingsactiviteiten gegevens medewerkers in Osiris

Verwerkingsactiviteiten gegevens medewerkers in Osiris		
Basisgegevensbeheer hoger onderwijs	Stagebegeleiding	Toetsbeoordeling
Onderzoeksregistratie	Identiteitgegevensbeheer	Toetsroosterconstructie
Autorisatiegegevensbeheer	Roosterpublicatie	Lesroosterconstructie
Onderwijsuitvoeringsbegeleiding	Toetsvoorbereidingsfunctie	Toetsuitvoering
Registratie en analyse gebruik app	Verslagen van begeleiding studenten door het decanaat	Verslaglegging psychologische ondersteuning
Inloggen	Registratie van agressie en geweld	Onderwijsactiviteitenplanning
Logging gebruiksgegevens	Analyse van studiegegevens	Analyse van agressie- en geweldsincidenten

Instellingen aanpassen	Registratie calamiteiteninformatie	Archivering en verwijdering
	Testen Osiris (indien met productiegegevens)	Meewerken aan opsporingsverzoeken
Support gebruik Osiris	Depersonaliseren van persoonsgegevens ten behoeve van testen	Kwalificatiecontrole
Digitaal portfolio		

4 Doelen van de verwerkingen

Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (artikel 5 (1), onder b AVG).

De algemene doelen van de verwerkingen in Osiris zijn gericht op de kerndoelen van de onderwijsinstellingen. Voor hogescholen en universiteiten is dit: het verzorgen van onderwijs en uitvoeren van wetenschappelijk onderzoek (zie artikel 1.3 lid 1 en lid 3 WHW). Op basis van dit kerndoel verwerken de instellingen in Osiris persoonsgegevens van de genoemde groepen betrokkenen.

De Wet educatie en beroepsonderwijs (WEB) omschrijft de doelstellingen van beroepsonderwijs als volgt:

> *"Beroepsonderwijs is gericht op de theoretische en praktische voorbereiding voor de uitoefening van beroepen, waarvoor een beroepskwalificerende opleiding is vereist of dienstig kan zijn. Het beroepsonderwijs bevordert tevens de algemene vorming en de persoonlijke ontplooiing van de deelnemers en draagt bij tot het maatschappelijk functioneren."* (artikel 1.2.1 lid 2 WEB).

In de Hoger Onderwijs Referentie Architectuur (HORA) wordt het studentinformatiesysteem (SIS) zoals Osiris gepositioneerd binnen het domein van 'onderwijsondersteuning'. Dit betekent dat het SIS een centrale rol speelt in het ondersteunen van onderwijsprocessen door het beheren en verstrekken van essentiële informatie over studenten en het onderwijsaanbod.

Binnen het 'Applicatiecomponentmodel' van de HORA is het SIS gedefinieerd als een 'referentieapplicatiecomponent'. Het wordt beschreven als een systeem dat het onderwijsaanbod en de belangrijkste gegevens van studenten administreert, inclusief hun studievoortgang.[19]

Applicatiemodel – Onderwijsondersteuning – SIS:[20]

- Onderwijsplanningsfunctie: Het ondersteunen van het koppelen van onderwijsaanbod aan deelnemers[21]
- Studievolgfunctie: Het ondersteunen van het volgen en begeleiden van deelnemers.[22]
- Studieinschrijffunctie: Het ondersteunen van het aanmelden, inschrijven en uitschrijven van deelnemers voor deelname aan (delen van) het onderwijsaanbod.[23]
- Onderwijsaanbodgegevensbeheer: Het beheren van gegevens over het onderwijsaanbod.[24]

[19] URL: https://hora.surf.nl/index.php/Id-feb2d938-5c98-62e7-d5fd-5da245ad6486.

[20] URL: https://hora.surf.nl/index.php/Id-903b3448-a486-b8e7-b94b-21f1d2276a30.

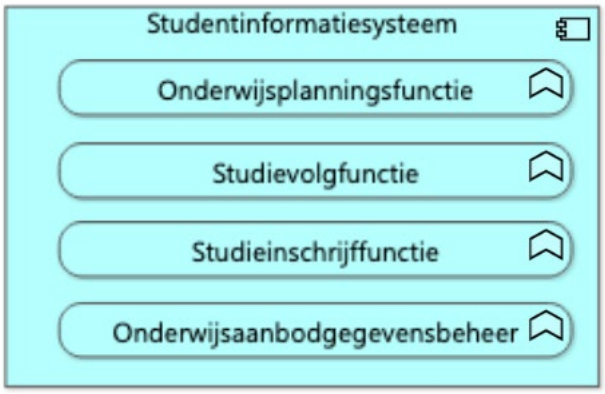
[21] URL: https://hora.surf.nl/index.php/Id-6436480e-be18-b3c6-284a-482c8d99e2dc.

[22] URL: https://hora.surf.nl/index.php/Id-833dfb78-91d5-b88e-7ae2-35e443915d57.

[23] URL: https://hora.surf.nl/index.php/Id-534614e9-14d1-04e3-1cd0-10ee7bc0bdbf.

[24] URL: https://hora.surf.nl/index.php/Id-4b3b1513-877d-013a-5941-4400a9807c3a

Figuur 3: Applicatiemodel SIS



De AVG vereist dat de verwerkingsdoelen voor iedere verwerking specifiek worden aangeduid. Daarvoor hebben de instellingen ieder een eigen verwerkingsregister ingericht en informeren zij ieder zelfstandig de betrokkenen over de verwerkingen via hun voorlichtingsmateriaal, zoals de privacyverklaring op de website. Deze specifieke doelen worden in deze DPIA niet beoordeeld, omdat zo'n beoordeling niet zou gaan over het gebruik van Osiris als systeem. Uiteindelijk worden de doelen per instelling bepaald. Wel is het van belang te constateren dat de doelen waarvoor de instellingen Osiris inzetten met betrekking tot verwerkingen die binnen scope van deze DPIA vallen allemaal direct gerelateerd moeten zijn aan de hoofddoelen.

De gegevens in Osiris kunnen gevoelig van aard zijn, wat hoge eisen stelt aan de informatiebeveiliging van het systeem. Instellingen kunnen hieraan gerelateerde doelen hebben, zoals het registreren van wijzigingen in het gebruik ten behoeve van verantwoording en correcte gegevensverwerking, evenals het vastleggen, monitoren en analyseren van het systeemgebruik met het oog op de beveiliging.

Volgens de bijlage bij de verwerkersovereenkomst van TiU betreft het doel van de verwerking *"de registratie van studentgegevens die voortvloeien uit de studentenadministratie en studiebegeleiding en alle daarmee samenhangende activiteiten."*

5 Verantwoordelijken, verwerkers en subverwerkers

Dit hoofdstuk geeft een overzicht van de betrokken partijen en hun rollen vanuit de AVG.

5.1 De onderwijsinstellingen

De instellingen (universiteiten, hogescholen en mbo-instellingen) die gebruik maken van de SaaS-applicatie van Osiris zijn onderwijsinstellingen die wetenschappelijk onderwijs, hoger onderwijs en middelbaar beroepsonderwijs verzorgen. De instellingen zijn ieder zelfstandig verwerkingsverantwoordelijke voor de gegevensverwerkingen in Osiris. Instellingen kunnen verschillende pakketten van de software afnemen met meer of minder modules. De instelling sluit daarbij een verwerkersovereenkomst met CACI B.V.

5.2 CACI B.V.

CACI B.V. is de leverancier en beheerder van Osiris. Het bedrijf ontwikkelt de Osiris-software en beheert de online cloudomgeving voor de instellingen. De hogescholen sluiten hiervoor een verwerkersovereenkomst af met CACI B.V. CACI B.V. is gecertificeerd conform ISO20000 (Service Management) voor haar werkprocessen en conform ISO27001 (Information Security Management) voor bedrijfsbrede security. Ook is CACI B.V. in het bezit van een ISAE 3402 Type II auditverklaring met betrekking tot de procesbeheersing voor Osiris SaaS.

CACI B.V. is verwerker voor de instellingen. Er zijn geen verwerkingen voor eigen doeleinden gevonden in het technisch onderzoek.

5.3 Subverwerkers CACI B.V.

CACI B.V. maakt gebruik van de volgende subverwerkers.

5.3.1 Interconnect

Interconnect levert aan CACI B.V. een Virtual Private Cloud en een Managed Firewall. In deze cloudopslag worden alle persoonsgegevens opgeslagen die binnen de SaaS-oplossing van CACI B.V. worden verwerkt.

CACI B.V. heeft in 2019 een subverwerkersovereenkomst met Interconnect gesloten, zoals volgens de AVG verplicht is.[25]

5.3.2 Microsoft

Back-ups worden versleuteld opgeslagen in de Azure cloud van Microsoft.

Om deze diensten te kunnen afnemen heeft CACI B.V. de standaard Data Processing Agreement van Microsoft afgesloten. Dit is de Microsoft Products and Services DPA.[26]

5.3.3 EnableU

EnableU levert aan CACI B.V. connections as a service, wat inhoudt dat een deel van de standaard koppelingen worden gefaciliteerd en beheerd.

---

[25] In de subverwerkersovereenkomst staat nog wel een (abusievelijke) verwijzing naar de WBP (Wet bescherming persoonsgegevens die in 2018 is vervangen door de AVG).

[26] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA, geraadpleegd op 7 augustus 2025.

CACI B.V. heeft in 2020 een subverwerkersovereenkomst met EnableU gesloten, zoals volgens de AVG verplicht is.[27]

5.4 Andere derde partijen

Naast de genoemde subverwerkers zijn de volgende partijen waargenomen tijdens het testen.

5.4.1 Google

Tijdens het testen zijn de volgende Google services aangetroffen (zie de Technische Appendix voor meer details):

- Google fonts op verschillende plaatsen in de web interface voor medewerkers.
- Firebase logging in de iOS App, hierbij werd er een device ID doorgestuurd naar Google.
- Firebase API key request in de Android App.
- Google Autofill in de Android App, hierbij wordt er een persoonlijke API-key meegestuurd.

Omdat TiU geen pushberichten gebruikt, was er geen Firebase Google Cloud Push push verbinding zichtbaar in de testresultaten. Het aanvragen van Firebase API key is wel de eerste stap daarvoor.

Daarnaast wordt de Osiris App voor Android standaard via de Google Play Store geïnstalleerd en heeft de Play Store ook toegang tot de lijst met geïnstalleerde apps. Daardoor heeft Google een link tussen het gebruik van de Osiris app en het Google-account van de student. Dit is niet specifiek voor de Osiris App, maar geldt voor alle apps die via de Play Store worden aangeboden.

5.4.2 Apple

Omdat TiU geen pushberichten gebruikt, was er geen Apple Push Notification push verbinding zichtbaar in de test resultaten.

Daarnaast wordt de Osiris App voor iOS via de Apple App-Store geïnstalleerd. Daardoor heeft Apple een link tussen het gebruik van de Osiris app en het Apple-account van de student. Dit is niet specifiek voor de Osiris App, maar geldt voor alle apps die via de Apple App-Store worden aangeboden.

5.5 Holdingstructuur CACI

CACI B.V. is 100% eigendom van CACI Holdings B.V. dat op haar beurt 100% eigendom is van het Engelse CACI Holdings Limited.[28] CACI Holdings Limited is opgericht op 23 december 2023[29] en is 100% eigendom van CACI International, Inc.

De twee Engelse bestuurders van CACI Holdings B.V. zitten samen met nog een Engelse en een Nederlandse bestuurder ook in het bestuur van CACI B.V. De twee Engelse bestuurders van CACI Holdings B.V. zitten samen met nog een Engelse bestuurder in het bestuur van de Engelse holding.

---

[27] In de subverwerkersovereenkomst staat nog wel een (abusievelijke) verwijzing naar de WBP (Wet bescherming persoonsgegevens die in 2018 is vervangen door de AVG).

[28] Uittreksel Kamer van Koophandel 27 maart 2025.

[29] https://find-and-update.company-information.service.gov.uk/company/15348070/filing-history, geraadpleegd op 11 april 2025.

Op 28 december 2023 is CACI N.V. gewijzigd (omgezet) in de huidige CACI Holdings B.V. Tot 29 december 2023 was CACI International Inc. de enige aandeelhouder van CACI N.V./CACI Holdings B.V.

Dat betekent dat tot 29 december 2023 de Nederlandse Holding rechtstreeks onder het Amerikaanse moederbedrijf viel. Tegenwoordig (sinds 29 december 2023) zit daar de Engelse Holding tussen.

CACI B.V. heeft een ‘Declaration of CACI B.V. relating to data processed as part of its Osiris software product/application’ opgesteld en gedeeld met SURF. In de bijlage is Artikel 14.3 van de statuten opgenomen waarin de bestuursbesluiten staan beschreven die een goedkeuring van de algemene vergadering vereisen. Deze statuten verwijzen niet naar operationele zaken.

De bovengenoemde verklaring stelt dat CACI B.V., direct noch indirect, enige persoonsgegevens uit Osiris deelt met CACI Holdings B.V., CACI Holdings Limited of CACI International Inc, en dat er geen overeenkomst bestaat die een dergelijke gegevensdeling toestaat.

6 Belangen bij de verwerking

6.1 De instellingen

Een studentinformatiesysteem (SIS) is een cruciaal en centraal onderdeel van de administratieprocessen van een onderwijsinstelling. Het belang van de instellingen bij het gebruik van een SIS is de efficiënte afhandeling van de bedrijfsvoering en voldoen aan de eisen van de verschillende relevante wetten, tegen zo laag mogelijke kosten. Keuzevrijheid in de systemen die ze gebruiken en controle over de gegevens in die systemen zijn daarbij van belang, net als continuïteit van de bedrijfsvoering en medewerkers- en studenttevredenheid. Daarnaast is het in het belang van de instellingen om zorgvuldig en rechtmatig om te gaan met de persoonsgegevens van de medewerkers en de studenten, onder andere om handhaving te voorkomen. Ten slotte hebben de instellingen een groot belang bij het onderhouden van hun reputatie als betrouwbare aanbieders van hoger onderwijs.

6.2 CACI B.V.

Voor CACI is het leveren van Osiris in het hoger onderwijs en middelbaar beroepsonderwijs een kerntaak. Osiris is in gebruik bij meer dan de helft van de Nederlandse instellingen voor hoger onderwijs, zo blijkt uit een notitie van Vereniging Samenwerkende Nederlandse Universiteiten VSNU uit 2021.

CACI heeft een (bedrijfs)belang om een dienst van hoge kwaliteit te leveren en de marktpositie te behouden, waarbij wordt voldaan aan de eisen van de Nederlandse wet- en regelgeving en heersende normen. Zo heeft CACI belang bij het passend beveiligen van het systeem en de data die daarin aanwezig is, het toepassen van dataminimalisatie en het ondersteunen van instellingen bij correct gebruik van Osiris. Daarbij staan kwaliteit, informatiebeveiliging en privacy centraal.

6.3 Subverwerkers

De subverwerkers Interconnect, EnableU en Microsoft hebben een commercieel belang bij het leveren van de diensten om CACI in staat te stellen om Osiris als SaaS-oplossing te leveren. Bovendien hebben zij een belang bij het voldoen aan wet- en regelgeving.

6.4 Overige partijen

Zoals beschreven in paragraaf 1.13 zijn bij de mobiele app Apple en Google als subverwerkers betrokken. Zij faciliteren onder meer het versturen van pushberichten. Het is onduidelijk of deze partijen ook persoonsgegevens voor eigen doeleinden verwerken. Daarnaast zijn Apple en Google betrokken bij de distributie van de mobiele app via hun app stores, waarbij gegevensverwerkingen plaatsvinden binnen hun eigen commerciële kaders en belangen.

6.5 Studenten

Studenten hebben belang bij een goed werkend en betrouwbaar SIS, waarbij de instelling zorgvuldig omgaat met gegevens in de studentenadministratie en de studieresultaten. Daarnaast hebben studenten een belang bij een discrete behandeling van informatie rond ziekte, bijzondere omstandigheden, studie-uitval en andere gevoelige informatie waarover de instelling kan beschikken, waarbij de instelling technische en organisatorische maatregelen treft om onbevoegd gebruik/toegang te voorkomen. Tot slot hebben studenten er belang bij dat hun eigen persoonsgegevens niet onnodig of onrechtmatig worden verwerkt in het systeem.

6.6 Medewerkers instellingen

Docenten en overig personeel hebben behoefte aan een goed werkend SIS, dat relevante informatie bevat over de studievoortgang en waarin efficiënt informatie over roosters, tentamens, cijfers, etc. kan worden ingevoerd en opgevraagd. Daarnaast hebben medewerkers er belang bij dat hun eigen persoonsgegevens niet onnodig of onrechtmatig worden verwerkt in het systeem.

7 Verwerkingslocaties

CACI B.V. mag de persoonsgegevens die in het kader van Osiris worden verwerkt conform de verwerkersovereenkomst met TiU niet doorgeven naar landen buiten de EER. De locaties van verwerkingen en de ingezette subverwerkers staan opgenomen in de verwerkersovereenkomst.

Interconnect verzorgt de housing en hosting van de gegevens die de instellingen in Osiris verwerken. Interconnect is gevestigd in Nederland en verzorgt de housing en hosting binnen Nederland. EnableU faciliteert de koppelingen tussen Osiris en externe systemen. EnableU is tevens gevestigd in Nederland en verzorgt deze diensten vanuit Nederland.

Osiris biedt in de subverwerkersovereenkomsten met Interconnect en EnableU wel de mogelijkheid voor doorgifte naar landen buiten de EER, mits is voldaan aan de wet- en regelgeving hieromtrent. In de verwerkersovereenkomst met TiU is dit dus beperkt en is dergelijke doorgifte uitgesloten zolang er geen voorafgaande schriftelijke toestemming vanuit TiU is.

Osiris maakt gebruik van Microsoft (Azure) voor de opslag van back-ups. De back-ups staan in Nederland. De contracten met Microsoft zijn gesloten met Microsoft Ireland als vertegenwoordiger voor Microsoft in de EER. Opslag van de gegevens (at rest) vindt op basis van de standaardovereenkomst van Microsoft plaats binnen de EER.

De back-ups kwalificeren als content data en vallen daarom binnen de afspraken van Microsoft over de EU Data Boundary.[30] Deze gegevens zijn dus uitgesloten van doorgifte naar landen buiten de EER. Uit de metadata, zoals de accountnaam waarmee de gegevens geüpload worden of het IP-adres vanaf waar de gegevens geüpload worden, zijn geen persoonsgegevens over de betrokkenen van Osiris te herleiden. Daardoor gaat het hierbij alleen om cloudopslag en is er geen sprake van telemetrie of andere diagnostische gegevens die buiten de reikwijdte van de EU Data Boundary vallen.

In het technisch onderzoek is bij de webinterface geen netwerkverkeer aangetroffen naar endpoints (van partijen) buiten de EER. De iOS App en de Android App maken beide gebruik van Google Firebase. De pushberichten in de app en het installeren van de app zijn bij de iOS App afhankelijk van Apple en bij de Android App afhankelijk van Google. Deze partijen verwerken gegevens ook buiten de EER. Dit betreft:

- Device ID
- Het Google-account indien de student bij Google ingelogd is met het device
- Een voor de universiteit unieke ID
- Een voor de installatie van de app unieke ID
- De inhoud van de pushberichten
- Het IP-adres van het apparaat

[30] Zie: https://learn.microsoft.com/nl-nl/privacy/eudb/eu-data-boundary-learn?culture=nl-nl&country=nl , laatst bezocht 5 juni 2025.

8 Bijzondere technieken en methoden

Bij het gebruik van Osiris door de onderwijsinstellingen is geen sprake van geautomatiseerde besluitvorming, profilering of big data verwerkingen.

9 Aanvullende wettelijke vereisten

Naast de AVG kan de volgende wet- en regelgeving van toepassing zijn bij het gebruik van Osiris door de onderwijsinstellingen.

Tabel 22: Aanvullende wet- en regelgeving

Afkorting	Wet- en regelgeving	Relevante artikelen (optioneel)
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek	7(1 en 3), 7(31)(e), 7(34), 7(39), 7(52)
WEB	Wet educatie en beroepsonderwijs	Hoofstuk 8
Wabb	Wet algemene bepalingen burgerservicenummer	10, 11, 12, 13
Wgbh/cz	Wet op Gelijke behandeling op grond van handicap of chronische ziekte	2, 4, lid f
AW	Archiefwet 1995 (inclusief Archiefbesluit 1995 en Archiefregeling)	5
	Selectielijst hogescholen/universiteiten	
	Selectielijst voor onderwijsinstellingen in het Middelbaar Beroepsonderwijs (mbo)	
BIHO	Baseline Informatiebeveiliging Hoger Onderwijs	N/A
WGBO/Wet BIG	Wet op de Geneeskundige Behandelovereenkomst en Wet op Beroepen Individuele gezondheidszorg.	Burgerlijk Wetboek, Boek 7, afdeling 5, Artikel 446 en verder

9.1 Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek

Bij het verzorgen van onderwijs vormt de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) het wettelijk kader voor hogescholen en universiteiten. De instellingen hebben een kwaliteitszorgsysteem, waarin onder meer het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor medewerkers en studenten nageleefd en toegepast.

9.2 Wet educatie en beroepsonderwijs

Bij het verzorgen van het onderwijs vormt de Wet educatie en beroepsonderwijs (WEB) het wettelijk kader voor mbo-instellingen. De instellingen hebben een kwaliteitszorgsysteem, waarin onder meer het zorgvuldig omgaan met gegevens in de studentenadministratie is geregeld. Daarnaast worden gedrags- en integriteitscodes voor medewerkers en studenten nageleefd en toegepast.

9.3 Wet algemene bepalingen Burgerservicenummer

Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het Burgerservicenummer (artikel 10 Wet algemene bepalingen Burgerservicenummer). Onderwijsinstellingen gelden in beginsel niet als overheidsorgaan, behalve wanneer zij taken van openbaar gezag hebben toegewezen gekregen.

9.4 Wet Gelijke behandeling op grond van handicap of chronische ziekte

Onderwijsinstellingen zijn door de Wet Gelijke behandeling op grond van handicap of chronische ziekte (Wgbh/cz) verplicht om naar gelang de behoefte doeltreffende aanpassingen te doen, tenzij dit voor hen een onevenredige belasting vormt.

9.5 Archiefwet 1995, Selectielijst hogescholen 2013 (actualisatie 2022), Selectielijst Universiteiten en Universitair Medische Centra 2020

Bij de uitvoering van hun werkzaamheden, vervullen hogescholen en universiteiten voor een beperkt aantal processen een openbaar gezagtaak. Openbaar gezagtaken vormen volgens artikel 5 AW de basis voor een selectielijst. Voor hogescholen is deze in 2013 opgesteld en in 2020 is voor universiteiten een selectielijst opgesteld die daarop gebaseerd is. Deze openbaar gezagtaken hebben voor de onderliggende selectielijsten grotendeels te maken met het wel of niet behalen van een graad door een student. Dit zijn de taken waarvoor de informatieobjecten vallen onder de werking van de Archiefwet 1995.

Deze taken zijn:

- Het afnemen van examens en het verstrekken van graden en getuigschriften (zie onder);
- Een geschil (bezwaar) gericht aan het bestuur, betreffende graadverstrekking;
- Een beroepschrift betreffende graadverstrekking, gericht aan het College van Beroep voor het hoger onderwijs (CBHO).

Bij de eerste taak moet worden opgemerkt dat alleen het besluit van het hogeschoolbestuur of het universiteitsbestuur voor verstrekking van de graad gezien kan worden als een openbaar gezagtaak, ingevolge een uitspraak van de Raad van State.[31]

Voor de openbaar gezagtaken geldt dat de selectielijst moet worden vastgesteld door de besturen van de hogescholen en op basis van artikel 5 AW, tevens door de minister van OCW. Bij de betreffende processen wordt aangegeven dat zij een openbaar gezagtaak in zich dragen en daarmee vallen onder de werkingssfeer van de Archiefwet 1995.

Betrokkenen kunnen rechten ontlenen aan de Selectielijst hogescholen per hogeschool, vanaf de vaststelling van de lijst bij die hogeschool. Als ingangsdatum voor de openbaar gezagtaken wordt

[31] 200507749/1 (uitspraak 19 juli 2006) van de Raad van State.

de inwerkingtreding van de WHW gehanteerd, te weten 8 oktober 1992. Informatieobjecten van vóór deze datum die blijk geven van de verstrekking van wettelijk beschermde titels (graden), dienen overeenkomstig te worden behandeld.

De Archiefwet vormt een uitzondering op de AVG. Dat houdt in dat persoonsgegevens in archieven bewaard mogen worden. Daarbij moet worden opgemerkt dat de persoonsgegevens alsnog verwijderd dienen te worden als deze niet nodig zijn voor de context van de zaak of dossier. De zaak of het dossier mag alleen relevante persoonsgegevens bevatten.[32]

9.6 Archiefwet 1995 & Selectielijst voor onderwijsinstellingen in het Middelbaar Beroepsonderwijs (mbo)

Bij de uitvoering van hun werkzaamheden, vervult een mbo-instelling voor een beperkt aantal processen een openbaar gezag taak. Openbare gezagtaken vormen volgens artikel 5 van de Archiefwet 1995 de basis voor een selectielijst. Deze taken hebben voor de onderliggende selectielijst grotendeels te maken met het wel of niet behalen van een graad door een student. Dit zijn de taken waarvoor de informatieobjecten vallen onder de werking van de Archiefwet 1995.

Enkele taken van mbo-instellingen kunnen worden aangemerkt als openbaar gezagtaken. In die gevallen raakt het besluit van het bevoegd gezag de rechtspositie van een leerling. De volgende openbaar gezagtaken kunnen worden onderscheiden:

- De afgifte van een getuigschrift.
- Het verlenen van vrijstelling op grond van de Leerplichtwet[33].

De Archiefwet vormt een uitzondering op de AVG. Dat houdt in dat persoonsgegevens in archieven bewaard mogen worden. Daarbij moet worden opgemerkt dat als de persoonsgegevens niet nodig zijn voor de context van de zaak of dossier, deze alsnog verwijderd dienen te worden. De zaak of het dossier mag alleen relevante persoonsgegevens bevatten.

9.7 Baseline Informatiebeveiliging Hoger Onderwijs (BIHO)

SURFibo heeft een model-informatiebeveiligingsbeleid ontwikkeld voor het hoger onderwijs. Het beleid gaat in op de relevante informatiebeveiliging maatregelen conform ISO 27002 die getroffen moeten worden in het hoger onderwijs.

9.8 WGBO / Wet BIG

Doordat de studentenpsychologen onder de wet beroepen individuele gezondheidszorg (Wet BIG) vallen, vallen ze ook onder de wet op de geneeskundige behandelovereenkomst (WGBO). De WGBO stelt:

> ***"Artikel 459***
> *1. De hulpverlener voert verrichtingen in het kader van de behandelingsovereenkomst uit buiten de waarneming van anderen dan de patiënt, tenzij de patiënt ermee heeft ingestemd dat de verrichtingen kunnen worden waargenomen door anderen.*
> *2. Onder anderen dan de patiënt zijn niet begrepen degenen van wie beroepshalve de*

[32] Artikel 5.2 Selectielijst hogescholen 2013, actualisatie 2022.

[33] Selectielijst voor onderwijsinstellingen in het Middelbaar Beroepsonderwijs (MBO). Selectielijst voor de administratieve neerslag van de openbaar gezagtaken van de zorgdragers over de periode vanaf 1 augustus 2017.

medewerking bij de uitvoering van de verrichting noodzakelijk is.
3. Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de verrichting op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door verrichtingen te doen waarnemen niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks niet toe."[34]

Daarmee vallen de notities van de studentenpsychologen niet alleen onder de gegevensbescherming van de AVG, maar ook onder het medisch beroepsgeheim zoals het is vastgelegd in diverse wetten en verdragen en moet de gegevensverwerking ook aan die vereisten voldoen. De Inspectie Gezondheidszorg en Jeugd hanteert de NEN7510-familie van normen als handhavingskader bij het beoordelen van de beveiliging van systemen die onder de WGBO vallen.

[34] Burgerlijk Wetboek. Boek 7 Bijzondere overeenkomsten, Titel 7 Opdracht, Afdeling 5 De overeenkomst inzake geneeskundige behandeling

10 Bewaartermijnen

Een verwerkingsverantwoordelijke mag persoonsgegevens bewaren, zolang deze nodig zijn voor het doel waarvoor ze werden verzameld, stelt de AVG (artikel 5 AVG). Daarna dient de verwerkingsverantwoordelijke de gegevens te vernietigen, tenzij de verwerkingsverantwoordelijke verplicht is deze langer te bewaren, bijvoorbeeld omdat dat in een wet is bepaald.

De volgende paragrafen beschrijven de bewaartermijnen in de bijlage van de verwerkersovereenkomst van TiU, de bewaartermijnen in Osiris en de bewaartermijnen zoals gehanteerd door Microsoft.

10.1 Bewaartermijnen in juridische documentatie

In de bijlage bij de verwerkingsovereenkomst van TiU, staat het volgende opgenomen met betrekking tot bewaartermijnen:

> *"Osiris beschikt over de functionaliteit om diverse bewaartermijnen per informatie object in te richten. De Verwerkingsverantwoordelijke draagt zelf de verantwoordelijkheid voor de naleving van de voor haar relevante wet- en regelgeving met betrekking tot de functionele inrichting van de bewaartermijnen.*
>
> *Osiris beschikt over de functionaliteit om verschillende autorisatieprofielen te definiëren en deze aan rollen te koppelen. Op deze manier kan de toegang tot (persoons)gegevens worden gelimiteerd voor eindgebruikers. Verwerkingsverantwoordelijke draagt zelf de verantwoordelijkheid voor het functioneel inrichten van deze profielen en rollen.*
>
> *De back-ups bij de verwerker kennen een beperkte bewaartermijn als omschreven in 4.12.5 van het document Standaard Dienstbeschrijving OSIRIS SaaS (november 2023)."*[35]

10.2 Gegevensverwijdering in Osiris

De onderwijsinstellingen zijn als verwerkingsverantwoordelijke zelf verantwoordelijk voor het juist inrichten van bewaartermijnen in Osiris met behulp van de daartoe aangeboden functionaliteiten. Als een onderwijsinstelling zelf gegevens verwijdert in Osiris blijven deze nog wel tijdelijk bewaard in de historie-database (zie paragraaf 1.6). De gegevens zijn dan echter direct niet meer zichtbaar in Osiris en niet inzichtelijk voor de normale gebruikers (studenten, docenten, etc.), maar alleen toegankelijk voor beheerders met toegang tot de historie-database. De bewaartermijnen voor de historiedatabases bepaalt iedere instelling afzonderlijk.

De bewaartermijnen van de back-ups zijn als volgt:

Tabel 23: bewaartermijnen verschillende soorten back-ups

Type back-up	Bewaartermijn
Server back up	7 dagen

[35] Verwerkersovereenkomst Tilburg University – CACI (OSIRIS), bijlage A.

Onsite Database ‘hot’ back up	14 dagen
Offsite database back-ups	
Dagelijks (incrementeel)	28 dagen
Wekelijks (volledig)	28 dagen
Maandelijks (volledig)	90 dagen
Kwartaal (volledig)	één jaar

10.3 Microsoft

Microsoft bewaart de gegevens die zij voor CACI B.V. verwerkt zo lang als de overeenkomst loopt en CACI B.V. niet zelf gegevens verwijdert. Na het aflopen van de overeenkomst wordt binnen 90 dagen het account verwijderd en binnen nog eens 90 dagen de nog opgeslagen klantgegevens.[36] In dit geval zijn dat de back-ups.

[36] Volgens de Microsoft Products and Services DPA (Jan 022024).

Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

11 Rechtsgrond

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (artikel 5, lid 1, onder a AVG). Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden (artikel 6, lid 1 AVG):

a) de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen
e) de verwerking is noodzakelijk voor de vervulling van een **taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Deze systeem DPIA richt zich op de verwerkingen die technisch mogelijk zijn of voortkomen uit de inrichting van Osiris. Onderwijsinstellingen dienen voor de verwerkingen die zij uitvoeren met behulp van de functionaliteiten van Osiris (zoals het koppelen van onderwijsaanbod aan deelnemers, het volgen en begeleiden van deelnemers, het aanmelden, inschrijven en uitschrijven van deelnemers) zelf te beoordelen of er per doel een toereikende rechtsgrond aanwezig is. Voor de verwerkingen in relatie tot het uitvoeren van de onderwijstaken zal de grondslag noodzakelijk voor het uitvoeren van een taak van algemeen belang zijn.

CACI treedt op als verwerker en handelt uitsluitend op basis van instructies van de onderwijsinstelling, die als verwerkingsverantwoordelijke optreedt. Er is niet gebleken dat CACI persoonsgegevens voor eigen doeleinden verwerkt. Omdat CACI de verwerking namens de onderwijsinstelling uitvoert, geldt de grondslag voor de verwerking die door de onderwijsinstelling wordt gebruikt ook voor CACI als verwerker.

12 Bijzondere en gevoelige persoonsgegevens

CACI treedt op als verwerker en verwerkt geen persoonsgegevens voor eigen doeleinden.

12.1 Bijzondere persoonsgegevens

Verwerkingsverantwoordelijken moeten een geldige uitzonderingsgrond uit artikel 9 AVG hebben voor de verwerking van bijzondere persoonsgegevens. Of de onderwijsinstellingen zich op een uitzonderingsgrond kunnen beroepen, valt buiten de scope van deze DPIA. Omdat CACI de verwerking van bijzondere persoonsgegevens namens de verwerkingsverantwoordelijke uitvoert, geldt voor CACI dezelfde uitzonderingsgrond als die de onderwijsinstelling hanteert.

In Osiris zijn geen velden opgenomen die specifiek vragen naar bijzondere persoonsgegevens. De standaard processen van onderwijsinstellingen waarvoor Osiris beoogt een ondersteunend platform te bieden, maken het echter wel waarschijnlijk dat bijzondere persoonsgegevens in Osiris worden verwerkt. In de module Student registreren onderwijsinstellingen of een student bijvoorbeeld extra tijd krijgt bij een tentamen vanwege dyslexie of de zaal kan verlaten wegens migraine.

In de module Inschrijving wordt voor internationale studenten de gegevensset vanuit de IND verwerkt. De vaste dataset van de IND bevat ook gegevens over een tuberculosetest. Dit zijn medische gegevens en daarmee bijzondere persoonsgegevens.

In Osiris slaan de onderwijsinstellingen een kopie van het identiteitsbewijs van de ingeschreven student op. Dit bevat gevoelige persoonsgegevens in de vorm van de pasfoto. De pasfoto kwalificeert hier echter niet als biometrische gegeven, omdat de verwerking niet plaatsvindt ten behoeve van unieke identificatie. Het gaat alleen om het verifiëren van de identiteit van de student.

Het is een keuze van de onderwijsinstellingen zelf of zij Osiris ook inzetten voor interacties tussen de student en de studentpsycholoog. Als dit gebeurt resulteert dit in een verwerking van bijzondere persoonsgegevens over gezondheid van de student en is hier een wettelijke uitzonderingsgrond voor nodig.

12.2 Nationale identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. Het gebruik van deze nummers dient met uiterste zorgvuldigheid plaats te vinden en de noodzaak om deze nummers te gebruiken dient goed onderbouwd te zijn (artikel 87 AVG en artikel 46 lid 1 UAVG). Bovendien vereist de Nederlandse wet dat het BSN alleen gebruikt mag worden door overheidsorganen, of door andere organisaties voor zover dat bij wet is voorgeschreven (volgens artikel 1 sub d Wet algemene bepalingen burgerservicenummer (Wabb)). Onderwijsinstellingen gelden in beginsel niet als overheidsorgaan, behalve wanneer zij taken van openbaar gezag hebben toegewezen gekregen.

Het PGN is het BSN, zoals bedoeld in artikel 1, sub b Wabb, of indien een student geen BSN kan verstrekken, het onderwijsnummer als bedoeld in artikel 8.1.1a, lid 4 WEB en artikel 7.31^{e}, lid 3

WHW. Indien een student (nog) geen BSN heeft maakt DUO een tijdelijk Onderwijsnummer aan voor die student.[37]

Onderwijsinstellingen zijn verplicht het PGN te op te nemen in hun administratie (art. 8.1.1a, lid 4 WEB en art. 7.39 lid 4 WHW). Zij gebruiken het BSN vervolgens onder meer voor de communicatie met onder meer DUO op grond van artikel 10 Wabb en bijvoorbeeld en daarnaast voor het administreren van financiële ondersteuning in uitzonderlijke gevallen (art. 7.51i WHW).

De WEB bevat ook bepalingen over het gebruik van het persoonsgebonden nummer van een leerling/student in het contact met een andere school of instelling voor ander onderwijs en voor de in- en uitschrijving van die leerling/student (art. 2.3.6a. lid 7 en 2.5.5a. lid 9 WEB).
Voor het opnemen van het BSN van studenten in de administratie bestaat dus een grondslag.

Een onderwijsinstelling heeft de optie om gebruik te maken van een externe service voor het ondertekenen van documenten. De onderwijsinstelling heeft daarbij de optie om de documenten te laten ondertekenen met DigID. In dat geval verstuurt Osiris het BSN van degene die ondertekent naar de ondertekenservice. Ondertekenen met DigID wordt op een beperkt aantal mbo-instellingen daadwerkelijk gebruikt. Mogelijkerwijs bestaat er geen grondslag voor deze verwerking van het BSN.

[37] Zie: https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs , laatst bezocht 6 juni 2025.

13 Doelbinding

Doelbinding is één van de kernbeginselen uit artikel 5 van de AVG. Het principe van doelbinding is dat gegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en niet verder mogen worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

De gegevens die onderwijsinstellingen in Osiris verwerken worden voor diverse doeleinden verzameld, zo blijkt uit de bronnen waar de gegevens vandaan kwamen tijdens het technisch onderzoek. Tijdens het onderzoek bij de TiU zijn er geen verwerkingen aangetroffen die niet in overeenstemming zijn met de doeleinden waarvoor de gegevens verzameld zijn. Onderwijsinstellingen kunnen met behulp van de verwerkingen in Osiris invulling geven aan de taken van algemeen belang, wettelijke verplichtingen en bedrijfsvoering om onderwijs te kunnen bieden. In beginsel worden de gegevens dus verwerkt voor de doeleinden waarvoor ze verzameld zijn en wordt voldaan aan het beginsel van doelbinding.

De externe koppelingen en de spiegeldatabase maken het mogelijk om de gegevens vanuit Osiris naar andere systemen over te brengen. Of deze systemen voldoen aan de doelbinding moet in de DPIA’s op deze systemen beoordeeld worden.

14 Noodzaak en evenredigheid

Alle gegevensverwerkingen moeten voldoen aan de beginselen van noodzaak en evenredigheid. Het begrip noodzaak bestaat uit twee samenhangende begrippen, namelijk proportionaliteit en subsidiariteit. De persoonsgegevens die worden verwerkt, moeten noodzakelijk zijn voor het doel van de verwerking. Proportionaliteit betekent dat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staat tot de verwerkingsdoeleinden. Subsidiariteit betekent dat de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, kunnen worden verwezenlijkt.

Evenredigheid betekent dat er een evenwicht is tussen de belangen van de betrokkene en de belangen van de verwerkingsverantwoordelijke. Een evenredige gegevensverwerking houdt in dat de hoeveelheid verwerkte gegevens niet buitensporig is in verhouding tot het doel van de verwerking. Als een verantwoordelijke zijn doel kan bereiken door minder persoonsgegevens te verwerken, moet hij de hoeveelheid verwerkte persoonsgegevens beperken tot wat noodzakelijk is. Daarom mag een verantwoordelijke alleen die persoonsgegevens verwerken die noodzakelijk zijn om het legitieme doel te bereiken. De toepassing van het beginsel van proportionaliteit is dus nauw verwant aan de beginselen van gegevensbescherming uit artikel 5 van de AVG.

14.1 Proportionaliteit: staat de verwerking in verhouding met het doel?

De kernvragen zijn: zijn de belangen goed afgewogen? En gaat de verwerking niet verder dan wat nodig is? Om te beoordelen of de verwerking in verhouding staat tot het belang van de verwerkingsverantwoordelijke(n), moet de verwerking voldoen aan de beginselen van artikel 5 van de AVG. Een verwerking is proportioneel als de inbreuk op de rechten en vrijheden van betrokkenen in verhouding staat tot het doel dat de verwerkingsverantwoordelijke nastreeft.

14.1.1 Rechtmatigheid, behoorlijkheid en transparantie

De gegevens moeten *"rechtmatig, eerlijk en transparant worden verwerkt ten opzichte van de betrokkene"* (artikel 5, lid 1, onder a) AVG). Dit betekent dat de betrokkenen op de hoogte moeten worden gebracht van de verwerking van hun gegevens, dat alle wettelijke voorwaarden voor gegevensverwerking worden nageleefd en dat het evenredigheidsbeginsel in acht wordt genomen.

Osiris als medisch dossier

Het zaaksysteem in Osiris kan voor diverse doeleinden worden ingezet. Onderwijsinstellingen laten hier in de praktijk ook de studentpsycholoog gebruik van maken. Daarmee komen snel bijzondere persoonsgegevens in Osiris te staan. Afhankelijk van het precieze gebruik kan het naast een afsprakensysteem ook gelden als administratie en mogelijk als patiëntendossier. In dat geval zijn aanvullende vereisten voor beveiliging van toepassing die niet zijn ingericht, omdat Osiris niet voor dergelijk gebruik bedoeld is. De keuze om Osiris ook door de studentpsycholoog te laten gebruiken ligt bij de onderwijsinstellingen.

Mobiele app

Naast de webinterface biedt CACI ook een mobiele app aan voor iOS en Android. Deze mobiele app is ontwikkeld met hetzelfde framework als de webinterface en biedt dezelfde functionaliteiten. Aanvullend biedt de mobiele app onderwijsinstellingen de mogelijkheid om

pushberichten te versturen naar studenten. De inhoud van deze berichten wordt door de onderwijsinstelling zelf bepaald en geconfigureerd.

Voor het versturen van pushberichten maakt de app gebruik van Apple Push Notications (APN) voor iOS en Firebase Google Cloud Push voor Android. Beide diensten vereisen dat de mobiele telefoon zich aanmeldt bij respectievelijk Apple of Google met een apparaat ID en een API-key. Deze unieke identifiers worden vervolgens gedeeld met de Osiris app, zodat pushberichten correct afgeleverd kunnen worden. Google kan dit combineren met het Google-account van de student als de student met het apparaat is ingelogd bij Google. Apple en Google verwerken in dit proces persoonsgegevens, zoals de voornoemde unieke identifiers die herleidbaar zijn tot individuele gebruikers. Deze partijen worden echter niet aangemerkt als (sub)verwerker in de verwerkersovereenkomst tussen CACI en de onderwijsinstelling. Ook worden de bijbehorende persoonsgegevens die via de mobiele app worden verwerkt niet gespecificeerd in de verwerkersovereenkomst.

Hierdoor ontbreekt transparantie over de verwerking, waardoor niet wordt voldaan aan het rechtmatigheidsbeginsel zoals bedoeld in artikel 5, lid 1 onder a van de AVG. Daarnaast wordt niet voldaan aan de vereisten van artikel 28 van de AVG met betrekking tot het inschakelen van (sub-)verwerkers.

14.1.2 Minimale gegevensverwerking

Het beginsel van dataminimalisatie houdt in dat de persoonsgegevens toereikend moeten zijn, ter zake dienend en er niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk voor het bereiken van het doel van de verwerking (artikel 5, lid 1 onder c AVG). Van elk persoonsgegeven dient te worden vastgesteld dat het noodzakelijk is.

Bij verschillende processen in Osiris, met name in de module ‘zaak’, kunnen studenten en medewerkers documenten uploaden. Dit kan bijvoorbeeld een onderbouwing zijn bij een verzoek om vrijstelling aan de examencommissie, maar ook bij het aanvragen van een verblijfsvergunning of een voorziening moeten studenten vaak diverse documenten aanleveren. Deze documenten kunnen gevoelige informatie bevatten en in sommige gevallen kan zelfs de bestandsnaam gevoelige persoonsgegevens prijsgeven. Uit het inzageverzoek van het student testaccount blijkt dat bestandsnamen zichtbaar zijn in de applicatieserverlogs. In dit specifieke geval had de student een diploma gedownload waarin zijn persoonsgegevens in de bestandsnaam stonden vermeld. Applicatieserverlogs dienen primair voor het bijhouden van systeem- en foutmeldingen en het monitoren van de werking van de applicatie. Door bestandsnamen te loggen in de applicatieserverlogs worden meer persoonsgegevens verwerkt dan noodzakelijk voor het bereiken van het doel van de verwerking. Dit is dan ook in strijd met het beginsel van dataminimalisatie.

14.1.3 Juistheid

De nauwkeurigheid van persoonsgegevens vormt een integraal onderdeel van gegevensverwerking. De AVG stelt dat de verwerkingsverantwoordelijke alle redelijke maatregelen moet nemen om ervoor te zorgen dat de gegevens correct en actueel zijn (artikel 5, lid 1, onder d) AVG). Osiris ondersteunt dit beginsel door koppelingen met ander systemen aan te bieden, waarmee handmatige invoer en de kans op invoerfouten worden beperkt. Als gegevens toch onjuist zijn, biedt Osiris functionaliteiten om deze te corrigeren. Er zijn geen technische of functionele beperkingen binnen Osiris aangetroffen die onderwijsinstellingen hinderen in het naleven van het juistheidsbeginsel.

14.1.4 Opslagbeperking

Het beginsel van opslagbeperking houdt in dat de persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is (artikel 5, lid 1, onder e AVG). Dit wil zeggen dat, zodra persoonsgegevens niet langer nodig zijn voor het doel van de gegevensverwerking, deze gegevens verwijderd of geanonimiseerd moeten worden, zodat deze in ieder geval niet meer herleidbaar zijn tot een specifiek persoon. Osiris biedt functionaliteiten waarmee onderwijsinstellingen dit beginsel kunnen naleven, zoals de mogelijkheid bewaartermijnen in te stellen en het geautomatiseerd verwijderen van persoonsgegevens. De onderwijsinstelling bepaalt zelf, op basis van de eigen selectielijsten, hoelang persoonsgegevens bewaard blijven. Osiris faciliteert naleving van het beginsel van opslagbeperking. Het is aan de onderwijsinstelling om hier zorgvuldig gebruik van te maken.

Microsoft bewaart de gegevens die zij voor CACI B.V. verwerkt zo lang als de overeenkomst loopt en CACI B.V. niet zelf gegevens verwijdert. Na het aflopen van de overeenkomst wordt binnen 90 dagen het account verwijdert en binnen nog eens 90 dagen de nog opgeslagen klantgegevens.[38] Daarna blijven de back-ups, via het back-upschema, nog een jaar bewaard. In dit geval zijn dat de back-ups. Als CACI na het eindigen van de overeenkomst met de onderwijsinstelling de back-ups niet proactief verwijdert bij Microsoft, worden deze gegevens langer verwerkt dan noodzakelijk. CACI heeft hiervoor standaard opschoonprocedures ingesteld, waarin alle gegevens worden geschoond zodra de procedure in werking is gezet.

14.1.5 Integriteit en vertrouwelijkheid

Persoonsgegevens moeten verwerkt worden op een dusdanige manier dat passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5, lid 1, onder f AVG jo. artikel 32 lid 1 en 2 AVG).

<u>Toegangsrechten medewerkers onderwijsinstellingen</u>

Osiris ondersteunt een fijnmazige autorisatiematrix, waarbij rechten per rol, faculteit, afdeling, cursus of student zijn in te stellen. De onderwijsinstelling is zelf verantwoordelijk voor het correct inrichten en onderhouden van deze autorisaties. Bij de implementatie begeleidt CACI dit proces, maar daarna ligt het beheer volledig bij de instelling. Uit tests blijkt dat deze role-based toegang goed werkt: medewerkers hebben alleen toegang tot gegevens die passen bij hun functie. Osiris biedt hiervoor voldoende functionaliteit, mits de instelling de autorisatiematrix goed toepast en zorgt voor een werkinstructie om rechten tijdig aan te passen, bijvoorbeeld bij wijzigingen in mentorschap of aan het eind van het studiejaar.

<u>Toegangsrechten CACI medewerkers</u>

CACI is ISO 27001 gecertificeerd en laat elk jaar in- en externe audits uitvoeren hiervoor. Daarnaast wordt elk jaar een ISAE-audit uitgevoerd. Het ISAE-rapport van 17 oktober 2024 meldt één beperking: "*Vastgesteld dat de uitgegeven toegangsrechten niet worden beoordeeld aan de hand van de autorisatiematrix*."[39] Hierdoor bestaat het risico dat gebruikers toegangsrechten behouden die niet (langer) aansluiten bij hun rol, wat kan leiden tot onbevoegde toegang.

[38] Volgens de Microsoft Products and Services DPA (Jan 022024).

[39] CACI: International Standard on Assurance Engagements Report (ISAE) 3402 Type II Voor de Osiris SaaS dienstverlening Periode: 1 juli 2023 tot en met 30 juni 2024, Ref: R2409-07; 17 oktober 2024

Bijzondere en gevoelige persoonsgegevens

Artikel 32 van de AVG schrijft voor dat passende beveiligingsmaatregelen moeten worden getroffen om persoonsgegevens te beschermen, afgestemd op de risico's die de gegevensverwerking met zich meebrengt. Overweging 83 benadrukt daarbij dat de gekozen maatregelen moeten zorgen voor een passend beveiligingsniveau, bijvoorbeeld door het toepassen van encryptie.

De verwerking van bijzondere persoonsgegevens brengt aantoonbaar een verhoogd risico met zich mee. Hoewel Osiris daar oorspronkelijk niet voor bedoeld is, worden bepaalde modules er wel voor gebruikt (zie ook paragraaf 2.3 en hoofdstuk 12). Bijzondere persoonsgegevens kunnen daarbij zowel worden ingevoerd in open tekstvelden als voorkomen in geüploade bestanden. Ook het verwerken van het BSN brengt extra risico's met zich mee.

Zoals beschreven in paragraaf 1.8 is momenteel alleen encryptie op diskniveau en database niveau toegepast. Encryptie op veldniveau ontbreekt. Hierdoor is het mogelijk dat medewerkers die toegang hebben tot de database, bijvoorbeeld medewerkers van de onderwijsinstelling die data-analyse doen op een gerepliceerde database, of beheerders met database toegang, toegang hebben tot de inhoud van deze velden. Voor het beperken van deze risico's is het noodzakelijk dat voor bijzondere en gevoelige persoonsgegevens en het BSN extra maatregelen genomen worden, bijvoorbeeld door deze gegevens ook op veldniveau te versleutelen.

Koppelvlakken

In het kader van het integriteitsbeginsel is het essentieel dat gegevensuitwisseling met externe systemen op een gecontroleerde en betrouwbare manier plaatsvindt. Zoals beschreven in paragraaf 1.5.6 biedt Osiris twee standaard interfaces waarmee onderwijsinstellingen eigen integraties kunnen realiseren. Daarbij bepalen zij zelf het koppelvlak, dat toegang heeft tot alle data in de database. De onderwijsinstelling kan via standaardfilters, SQL-queries, aangepaste eigen voorwaarden ("alleen tonen als …"), het uitsluiten van kolommen (zoals het BSN) en de bestaande permissies nauwkeurig sturen welke gegevens worden gedeeld. Externe applicaties kunnen, indien nodig, ook gegevens naar Osiris sturen. (Toegang tot) deze interfaces is beveiligd met authenticatie. De ruime mogelijkheden die deze interfaces bieden, vragen om een zorgvuldige inrichting en duidelijke governance vanuit de onderwijsinstelling: de applicatie waaraan de gegevens overgedragen zijn en het gebruik van die applicatie moeten eenzelfde rechtenstructuur en governance hebben als Osiris. Als deze governance rondom de koppelvlakken niet goed geregeld is, bestaat het risico op onbevoegde toegang, datalekken of onrechtmatige gegevensverwerkingen.

Sleutelbeheer back-up

Zoals beschreven in paragraaf 1.8 versleutelt CACI alle database back-ups. Voor het sleutelbeheer, maakt CACI gebruik van de 'Oracle Secured Wallet' software. Deze software is ook gehost bij Interconnect. Het levert een risico op als de back-up sleutels in verkeerde handen vallen. Als de back-up sleutels in verkeerde handen vallen, dan zijn de versleutelde back-ups een relatief eenvoudig doelwit via waar de databases van Osiris achterhaald kunnen worden.
De (versleutelde) back-ups die bij Azure opgeslagen zijn, hebben daar een lager beschermingsniveau dan de oorspronkelijke gegevens op de infrastructuur bij Interconnect. Dat maakt de bescherming van de sleutels relevanter.

CACI maakt een back-up van de sleutels door deze met weer een andere sleutel te versleutelen en deze versleutelde sleutel in het versiebeheersysteem van de software op te nemen. Een partij of individu kan de back-ups van Osiris ontsleutelen als deze partij of individu:

1. Toegang heeft tot de versleutelde back-ups van Osiris **en** toegang heeft tot de sleutels waarmee de back-up versleuteld is.
2. Toegang heeft tot de versleutelde back-ups van Osiris **en** toegang heeft het versie beheersysteem waarin de versleutelde back-up sleutels worden bewaard **en** toegang heeft tot de sleutels waarmee de back-up van de back-up sleutels versleuteld is.

Aangezien de versleutelde sleutel wordt opgeslagen in het versiebeheersysteem, blijven deze versleutelde sleutels eindeloos bewaard. Deze zijn alleen ontoegankelijk te maken door de sleutel waarmee de sleutels versleuteld worden te wijzigen en de oude versies van die sleutel overal te wissen.

Spiegeldatabase

Osiris biedt onderwijsinstellingen de mogelijkheid om een (read only) replicatie van de database te maken en te exporteren naar een eigen server. Hierdoor kunnen zij direct via SQL of tools zoals PowerBI de gegevens bevragen en ook doorsturen naar een datalake voor verdere analyse en verwerking. Hoewel de replicatiefunctie zelf geen risico's met zich meebrengt, kan onvoldoende governance door de onderwijsinstelling wel leiden tot risico's, zoals disproportionele toegang, het niet naleven van bewaartermijnen, onrechtmatige verwerking, onvoldoende authenticatie of ongeoorloofde toegang tot bijzondere persoonsgegevens (artikel 9 AVG), bijvoorbeeld door onvoldoende toezicht op de data-analyses en het gebruik daarvan.

14.2 Subsidiariteit: is er een minder ingrijpende oplossing voorhanden?

Een verwerking voldoet aan het beginsel van subsidiariteit als er geen minder ingrijpende methode beschikbaar is om hetzelfde doel te bereiken. De hamvraag is of dezelfde doelen bereikt kunnen worden met minder inbreuk makende middelen.

De mobiele app van Osiris is beschikbaar via de Apple App Store en de Google Play Store. Wanneer een student de app downloadt, ontstaat er automatisch een koppeling tussen het gebruik van de app en het persoonlijke Apple- of Google-account van de student. Deze platformen krijgen daardoor inzicht in het feit dat de app is geïnstalleerd, wat kan leiden tot indirecte identificatie van de onderwijsinstelling van de student. Deze vorm van gegevensverwerking is niet strikt noodzakelijk voor het aanbieden van de app, aangezien minder privacy-invasieve alternatieven bestaan. Zo zou CACI ervoor kunnen kiezen om de app als zogeheten "sideload" aan te bieden buiten de reguliere appstores om, waardoor de betrokkenheid van Google en Apple worden geminimaliseerd. Gezien er minder ingrijpende mogelijkheden beschikbaar zijn, voldoet CACI aan het subsidiariteitsbeginsel.

De mobiele Osiris app verzendt pushberichten. De pushberichten veroorzaken zowel de overdracht van metadata en inhoud aan Google en Apple. De metadata betreft gegevens als device identifyers, IP-adressen en mogelijkerwijs het Google-account van de student. De inhoud betreft de berichten indien die inhoud onversleuteld verstuurd wordt, zoals noodzakelijkerwijs het geval is bij het 'notification messages' deel van de push berichten. De inhoud daarvan is zichtbaar voor en wordt verwerkt door Google. Onderwijsinstellingen bepalen zelf de inhoud van de berichten en kunnen daarin privacyvriendelijke keuzes maken, bijvoorbeeld door geen persoonsgegevens op te nemen. Ongeacht de inhoud van de berichten, wordt door het gebruik van notification messages de inhoud van de berichten structureel verwerkt door Google. Het is

mogelijk om dit te reduceren door gebruik te maken van een encrypted data payload, al dan niet boven op de notification message. Indien een student Unified Push, een alternatieve push infrastructuur voor Android, beschikbaar heeft, dan kan de app daar ook gebruik van maken en terugvallen op Google als het niet beschikbaar is. Gezien de afwezigheid van beide mitigerende maatregelen, wordt met het gebruik van notification messages niet voldaan aan het subsidiariteitsvereiste.

15 Rechten van betrokkenen

Betrokkenen hebben onder de AVG diverse rechten met betrekking tot hun persoonsgegevens. Dit betreft onder andere het recht op inzage, rectificatie en het recht op gegevenswissing (vergetelheid). In dit hoofdstuk wordt enkel ingegaan op de vraag in hoeverre onderwijsinstellingen met Osiris kunnen voldoen aan de verzoeken van betrokkenen, waarbij ook wordt besproken hoe de technische en organisatorische inrichting van het systeem invloed heeft op het daadwerkelijk kunnen uitvoeren van de rechten van betrokkenen. Het uitvoeren van het recht op beperking van de verwerking (artikel 18 AVG) en het recht om bezwaar te maken (artikel 21 AVG) zal in de praktijk resulteren in het rectificeren en wissen van gegevens. Daarom worden deze niet apart besproken in dit hoofdstuk. Er vindt geen automatische besluitvorming plaats in Osiris.

15.1 Recht op informatie

Het recht op transparante informatie (artikel 12 AVG) houdt in dat betrokkenen op een begrijpelijke en toegankelijke manier moeten worden geïnformeerd over de verwerking van hun persoonsgegevens. Dit stelt hen in staat om hun rechten onder de AVG effectief uit te oefenen.

Er ontbreekt essentiële informatie over de verwerkingen met betrekking tot de mobiele app: de verwerkte persoonsgegevens en de betrokken subverwerkers worden niet vermeld in de verwerkersovereenkomst. Hierdoor kan de onderwijsinstelling als verwerkingsverantwoordelijke betrokkenen niet op transparante wijze informeren over de gegevensverwerking.

Onderwijsinstellingen die de mobiele Osiris app aanbieden aan hun studenten kunnen op dit moment niet voldoen aan hun transparantieverplichting onder de AVG.

15.2 Recht op inzage

Het recht op inzage (artikel 15 AVG) geeft betrokkenen het recht om te weten welke persoonsgegevens over hen worden verwerkt en om hiervan een kopie te ontvangen.

Een betrokkene kan in Osiris direct zelf zijn persoonsgegevens inzien via de gebruikersinterface. Voor gegevens die niet direct zichtbaar zijn, zoals bepaalde loggegevens (auditlogs), kunnen beheerders een beperkt overzicht raadplegen. Indien aanvullende informatie nodig is, zoals applicatielogs, biedt CACI ondersteuning om deze gegevens op verzoek (supportverzoek) van de onderwijsinstelling te verstrekken, zodat de onderwijsinstelling in staat is om het inzageverzoek van de betrokkene in te willigen.

Met Osiris en (indien nodig) de medewerking van CACI kan de onderwijsinstelling effectief voldoen aan de AVG-verplichtingen voor inzageverzoeken, mits de eigen interne processen op orde zijn om de verzoeken af te handelen.

15.3 Recht op rectificatie

Betrokkenen hebben recht op rectificatie van onjuiste of onvolledige persoonsgegevens (artikel 16 AVG). Osiris bevat geen technische of functionele beperkingen die onderwijsinstellingen belemmeren bij het honoreren van rectificatieverzoeken en het aanpassen van persoonsgegevens.

15.4 Recht op gegevenswissing

Betrokkenen hebben op grond van artikel 17 AVG het recht op gegevenswissing, wat betekent dat zij onder bepaalde voorwaarden kunnen verzoeken dat hun persoonsgegevens worden verwijderd. Dit geldt bijvoorbeeld wanneer de gegevens niet langer nodig zijn, de toestemming is ingetrokken of de verwerking onrechtmatig is. Een dergelijk verzoek kan een deel van de gegevens van een betrokkene betreffen, bijvoorbeeld als een bepaalde notitie onrechtmatig bleek (gedeeltelijke verwijdering), of alle gegevens van de betrokkene (complete verwijdering).

Wanneer een student een verwijderverzoek indient bij de onderwijsinstelling, en de student een gedeeltelijke verwijdering van de gegevens verzoekt, dan worden deze gegevens in Osiris verwijderd uit de normale databasetabellen en historietabellen, waarbij alleen nog tijdelijke loggegevens of wijzigingshistorie kunnen achterblijven totdat de ingestelde bewaartermijn daarvan verloopt en een volledige opschoning plaatsvindt (zie ook paragraaf 1.11). Afhankelijk van wat er in de wijzigingshistorie is vastgelegd, kan het dus voorkomen dat er nog persoonsgegevens tijdelijk bewaard blijven, waardoor de onderwijsinstelling mogelijk niet volledig aan het verwijderverzoek voldoet zolang die gegevens nog herleidbaar zijn en niet zijn opgeschoond.

Indien de student een complete verwijdering verzoekt, en de onderwijsinstelling voert dit uit met de functie voor het verwijderen van een student, dan worden de gegevens ook uit de historietabellen verwijderd en worden een aantal gegevens die om technische of administratieve redenen niet verwijderd kunnen worden gepseudonimiseerd. Deze pseudonimisering is alleen met een excessieve inspanning te herleiden naar de oorspronkelijke student.

Bij een verwijderverzoek zullen ook de persoonsgegevens nog in de verschillende back-ups terug te vinden zijn. De back-ups zijn versleuteld en zolang er geen restore dient plaats te vinden, worden deze gegevens niet actief verwerkt of geraadpleegd en worden ze geschoond na het aflopen van de bewaartermijn.

Gegevens zijn dus op twee manieren te verwijderen:

1. Met de ‘wis student’ functie. In dat geval bevat alleen de back-up nog de gegevens van de student. Deze back-up blijft een jaar bewaard.
2. Door selectief te verwijderen. In dat geval bevatten de historie tabellen nog de geschiedenis van de gegevens. Deze historie wordt na de bewaartermijn, die per tabel kan wisselen, automatisch verwijderd. Ook bevat de back-up de gegevens. Deze worden een jaar bewaard.

15.5 Recht op dataportabiliteit

Het recht op dataportabiliteit houdt in dat betrokkenen het recht hebben om hun persoonsgegevens te laten overdragen (artikel 20 AVG). Osiris bevat geen technische of functionele beperkingen die onderwijsinstellingen belemmeren bij het honoreren van verzoeken om dataportabiliteit (indien de betrokkene daarvoor in aanmerking komt).

Deel C: Beschrijving en beoordeling risico’s voor de betrokkenen

Het verwerken van persoonsgegevens leidt vrijwel altijd tot enige risico’s voor de rechten en vrijheden van de betrokkenen. Dat geldt ook voor Osiris. Deel C van deze DPIA beschrijft de mogelijke risico’s die op kunnen treden en beoordeelt op basis van de mogelijke impact van de risico’s op de rechten en vrijheden van de betrokkenen en de kans dat het risico zich voor kan doen of het gaat om lage of hoge risico’s.

16 Risico's

Een DPIA gaat over de risico's voor betrokkenen, dus niet zozeer over de beveiligingsrisico's, continuïteitsrisico's of andere risico's die de organisatie die de DPIA uitvoert loopt. Dit maakt de insteek verwant aan die van andere vakgebieden, maar is deze toch fundamenteel anders dan de risicoanalyses uit die andere vakgebieden. De verwantschap is echter wel sterk. Een inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens kan, als het persoonsgegevens betreft, ook resulteren in een privacyrisico.

In dit hoofdstuk worden de risico's bepaald en onderzocht wat de kans op en gevolgen van de risico's zijn. In Deel D volgen de maatregelen waarmee de risico's eventueel beperkt (gemitigeerd) kunnen worden.

De Engelse toezichthouder ICO heeft een lijst met hoofdcategorieën van risico's opgesteld:[40]

- Verlies van controle op het gebruik van de gegevens
- Verlies van vertrouwelijkheid
- Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen
- Heridentificatie van gepseudonimiseerde gegevens

Op basis van deze algemene lijst met risico's kunnen de specifieke risico's binnen deze DPIA worden vastgesteld en vervolgens worden weergegeven in een zogenaamde risicomatrix. Zie daarvoor het figuur hieronder. De uitkomst (het risico) wordt bepaald aan de hand van de gevolgen (minimaal, enige, ernstige) en de kans (heel klein, redelijke mogelijkheid, waarschijnlijker dan niet). De invulling van de kans en de gevolgen vraagt een inschatting.

Tabel 24: Risico Matrix

Ernst van de gevolgen voor de betrokkene(n)	Ernstige gevolgen	Laag risico	Hoog risico	Hoog risico
	Enige negatieve gevolgen	Laag risico	Medium risico	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

Bij het bepalen van de risico's zijn de volgende criteria toepasselijk:

Kans dat het risico zich voordoet

[40] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/, geraadpleegd op 18 juli 2025

- Heel klein: Het is onwaarschijnlijk dat dit risico zal optreden.
- Redelijke mogelijkheid: Het is denkbaar dat dit risico zal optreden.
- Waarschijnlijker dan niet: Het is waarschijnlijk of zeker dat het risico zal optreden.

Ernst van de gevolgen

- Minimale gevolgen: Als het risico zich voordoet heeft dit weinig of geen gevolgen voor de rechten en vrijheden van betrokkene
- Enige negatieve gevolgen: Als het risico zich voordoet heeft dit enige invloed op de rechten en vrijheden van betrokkene
- Ernstige gevolgen: Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene

Indien door een risico een fundamenteel beginsel van de AVG wordt geschonden, wordt de impact altijd als hoog ingeschat, aangezien dit direct een inbreuk vormt op de rechten en vrijheden van de betrokkene.

16.1 Risico-inventarisatie

Bij de uitvoering van deze DPIA zijn de volgende risico's geïdentificeerd:

Tabel 25: Risico-inventarisatie

#	Risico	Categorie risico	Kans	Impact
1.	Osiris als administratie studentpsycholoog	Onrechtmatige verwerking (oneigenlijk gebruik van Osiris)	Redelijke mogelijkheid	Ernstige gevolgen
2.	Verwerking van BSN bij digitaal ondertekenen met DigID heeft mogelijk geen wettelijke grondslag	Onrechtmatige verwerking BSN	Niet beoordeelbaar	Ernstige gevolgen
3.	Bestandsnamen in applicatieserverlogs	Gebrek aan dataminimalisatie	Waarschijnlijker dan niet	Ernstige gevolgen
4.	Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI)	Verlies van vertrouwelijkheid	Redelijke mogelijkheid	Ernstige gevolgen
5.	Geen veldniveau-encryptie bij bijzondere of gevoelige persoonsgegevens	Verlies van vertrouwelijkheid	Redelijke mogelijkheid	Ernstige gevolgen
6.	Onvoldoende governance koppelvlakken	Verlies van vertrouwelijkheid	Redelijk mogelijkheid	Ernstige gevolgen

7.	Onvoldoende governance spiegeldatabase functionaliteit	Verlies van controle op het gebruik van de gegevens	Redelijke mogelijkheid	Ernstige gevolgen
8.	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd	Verlies van vertrouwelijkheid	Redelijke mogelijkheid	Enige gevolgen
9.	Back-ups langer verwerkt dan nodig bij beëindigen contract	Verlies van controle op het gebruik van de gegevens	Redelijke mogelijkheid	Ernstige gevolgen
Risico's verbonden aan de mobiele app				
10.	Onvoldoende transparantie over mobiele app	Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen	Redelijke mogelijkheid	Ernstige gevolgen
11.	Mobiele app niet als 'side-load' beschikbaar	Verlies van controle op het gebruik van de gegevens	Waarschijnlijker dan niet	Ernstige gevolgen
12.	Pushberichten verzonden als 'notification messages'	Verlies van controle op het gebruik van de gegevens	Waarschijnlijker dan niet	Ernstige gevolgen
13.	Verwerkersovereenkomsten onvolledig m.b.t. mobiele app	Verlies van controle op het gebruik van de gegevens	Waarschijnlijker dan niet	Ernstige gevolgen

Hieronder volgt een korte toelichting van de risico's.

16.1.1 Risico 1: Osiris als administratie studentpsycholoog

Het zaaksysteem in Osiris kan voor diverse doeleinden worden ingezet. Onderwijsinstellingen laten hier in de praktijk ook de studentpsycholoog gebruik van maken. Daarmee komen snel bijzondere persoonsgegevens in Osiris te staan. Afhankelijk van het precieze gebruik kan het naast een afsprakensysteem ook gelden als administratie en mogelijk als patiëntendossier. In dat geval zijn aanvullende vereisten voor beveiliging van toepassing die niet zijn ingericht, omdat Osiris niet voor dergelijk gebruik bedoeld is. Een van die punten is het voldoen aan de NEN-7510 familie van veiligheidsnormen. De NEN-7510 eist onder andere dat de risicoanalyse voor het beveiligingsbeheer expliciet rekening houdt met de verwerking van gezondheidsgegevens en gegevens die onder de WGBO vallen. De keuze om Osiris ook door de studentpsycholoog te laten gebruiken ligt bij de onderwijsinstellingen.

De kans dat dit risico zich voordoet is redelijk aanwezig, er zijn onderwijsinstellingen die Osiris zo inzetten. Indien het risico zich voordoet en leidt tot verwerkingen waarbij de wettelijk vereiste waarborgen niet zijn ingericht zijn de gevolgen voor de rechten en vrijheden van betrokkenen ernstig. Dit kwalificeert als een **hoog risico**.

16.1.2 Risico 2: Verwerking van BSN bij digitaal ondertekenen met DigID heeft mogelijk geen wettelijke grondslag

De onderwijsinstelling kan ervoor kiezen om documenten te laten ondertekenen met de DigiD module. In dat geval wordt echter een extra verwerking van het BSN uitgevoerd. Het is ten tijde van het schrijven van deze DPIA onduidelijk in welke gevallen er een wettelijke grondslag bestaat voor deze verwerking van het BSN, terwijl er een alternatief beschikbaar is in Osiris waarbij deze extra verwerking van het BSN niet vereist is. Zie 1.5.3 Digitaal ondertekenen.

Een aantal onderwijsinstellingen maakt gebruik van deze functie. De beoordeling van de aanwezigheid van een grondslag voor het gebruik van het BSN, is echter aan die onderwijsinstellingen zelf. Daardoor is het onbekend in hoeverre het BSN zonder grondslag verwerkt wordt. Omdat deze DPIA niet kan bevestigen dat deze verwerkingen plaatsvinden met een wettelijke grondslag, is de kans dat het gebeurt in het kader van deze DPIA als 'redelijk aanwezig' bepaald. De gevolgen voor de rechten en vrijheden van betrokkenen zijn groot. Er is immers een alternatief, waardoor in dit geval niet is voldaan aan het subsidiariteitsbeginsel. Dit kwalificeert als een **hoog risico**.

16.1.3 Risico 3: Bestandsnamen in applicatieserverlogs

Bij verschillende processen in Osiris, met name in de module 'zaak', kunnen studenten en medewerkers documenten uploaden die gevoelige informatie bevatten. Bestandsnamen van deze documenten, waarin soms persoonsgegevens staan, worden zichtbaar gelogd in de applicatieserverlogs. De applicatielogs zijn alleen toegankelijk voor systeembeheerders van CACI. Door het opnemen van bestandsnamen in applicatielogs worden meer persoonsgegevens verwerkt dan noodzakelijk, wat in strijd is met het dataminimalisatiebeginsel.

Dit is een bestaande situatie, dus de kans dat dit risico zich voordoet is waarschijnlijker dan niet. De gevolgen voor de rechten en vrijheden van betrokkenen zijn ernstig, aangezien dit een verwerking oplevert die in strijd is met het beginsel van dataminimalisatie. Persoonsgegevens worden hierdoor mogelijk inzichtelijk voor systeembeheerders, terwijl die geen toegang tot deze gegevens hoeven te hebben. Dit kwalificeert als een **hoog risico**.

16.1.4 Risico 4: Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI)

Technisch beheerders van CACI hebben toegang tot alle categorieën persoonsgegevens binnen Osiris. Zij mogen deze gegevens inzien, maar mogen wijzigingen alleen uitvoeren met expliciete toestemming van de onderwijsinstelling. Ook hebben sommige beheerders toegang tot de sleutel waarmee de back-up-keys versleuteld zijn. Uit het ISAE-rapport van 2024 blijkt dat CACI-toegangsrechten niet structureel beoordeelt op basis van een actuele autorisatiematrix. Hierdoor bestaat het risico dat medewerkers van CACI toegangsrechten behouden die niet (langer) aansluiten bij hun rol, wat kan leiden tot toegang tot persoonsgegevens die buiten hun functionele verantwoordelijkheid vallen. Volgens CACI is het proces sinds de vorige ISAE audit structureel gewijzigd. Bij de komende ISAE-audit (augustus 2025) zal dit getoetst worden.[41]

CACI heeft diverse technische en organisatorische beveiligingsmaatregelen getroffen, die ook zijn vastgelegd in de verwerkersovereenkomst. Deze maatregelen verkleinen de kans op misbruik, maar sluiten onbedoelde toegang niet volledig uit. Omdat toegangsrechten niet actief worden getoetst aan een actuele autorisatiematrix, is er een redelijke mogelijkheid dat dit risico

[41] Feedback CACI 11 juni 2025.

zich voordoet. Mocht het risico zich voordoen, dan kan dit ernstige gevolgen hebben voor de rechten en vrijheden van betrokkenen, aangezien er sprake is van verlies van vertrouwelijkheid van persoonsgegevens. Gelet op de waarschijnlijkheid en impact is dit een **hoog risico**.

16.1.5 Risico 5: Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens

CACI past momenteel encryptie op diskniveau en op databaseniveau toe. Encryptie op veldniveau ontbreekt nog. Hierdoor zijn bijzondere persoonsgegevens en andere gevoelige gegevens, zoals het BSN, binnen Osiris niet aanvullend beschermd, ondanks het hogere risico dat verwerken van deze gegevens met zich meebrengt.

In Osiris zijn geen velden opgenomen die specifiek vragen naar bijzondere persoonsgegevens. De standaard processen van onderwijsinstellingen waarvoor Osiris beoogt een ondersteunend platform te bieden impliceren echter wel dat bijzondere persoonsgegevens in Osiris worden verwerkt (zie ook paragraaf 2.3 en hoofdstuk 12). Deze gegevens worden zowel ingevoerd in vrije tekstvelden en notitievelden als geüpload in documenten. BSN's en PGN's worden in het kader van het onderwijs standaard verwerkt. Door het ontbreken van veldniveau-encryptie zijn deze persoonsgegevens niet beter beveiligd dan reguliere persoonsgegevens.

Dit betekent dat instellingen bestaande maatregelen goed moeten implementeren om de kans te verkleinen dat bijzondere persoonsgegevens en BSN's bij een datalek of onbevoegde toegang leesbaar zijn en direct schade kunnen veroorzaken. Denk bijvoorbeeld aan identiteitsfraude. Dit speelt bij onrechtmatige toegang tot de databases van Osiris, maar ook bij het overdragen van deze gegevens aan andere systemen zoals bij de externe koppelingen en de schaduwdatabase. Encryptie op veldniveau maakt het ook voor die systemen mogelijk om de toegang te beperken door de sleutel maar beperkt beschikbaar te maken. CACI hanteert wel algemene beveiligingsmaatregelen zoals toegangsbeperking en logging.

Er is een redelijke mogelijkheid dat onbevoegde toegang plaatsvindt, bijvoorbeeld via een technische kwetsbaarheid of misbruik van rechten. Gezien de aard van de gegevens en de ernst van de mogelijke gevolgen die inherent is aan verwerkingen met bijzondere persoonsgegevens levert dit een **hoog risico** op.

16.1.6 Risico 6: Onvoldoende governance koppelvlakken

Als door de onderwijsinstellingen de governance rondom de koppelvlakken niet goed geregeld is, bestaat het risico op onbevoegde toegang, datalekken of onrechtmatige gegevensverwerkingen.

Hoewel de governance van de functionaliteit volledig onder de verantwoordelijkheid van de onderwijsinstelling valt en deze functionaliteit zelf geen risico's binnen Osiris met zich meebrengt, wordt het risico hier wel benoemd zodat onderwijsinstellingen zich bewust zijn van mogelijke aandachtspunten. Er is een redelijke mogelijkheid dat een van de voornoemde risico's zich voordoet. Als een van de risico's zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene. Om die reden kwalificeert dit als een **hoog risico**.

16.1.7 Risico 7: Onvoldoende governance spiegeldatabase functionaliteit

Osiris biedt onderwijsinstellingen de mogelijkheid om een (read-only) replicatie van de database te maken en te exporteren naar een eigen server. Hierdoor kunnen zij direct via SQL of tools zoals PowerBI de gegevens bevragen en ook doorsturen naar een datalake voor verdere analyse en verwerking. Hoewel deze functionaliteit zelf geen risico's met zich meebrengt, kan

onvoldoende governance door de onderwijsinstelling wel leiden tot risico's, zoals disproportionele toegang, het niet naleven van bewaartermijnen, onrechtmatige verwerking, onvoldoende authenticatie of ongeoorloofde toegang tot bijzondere persoonsgegevens (artikel 9 AVG).

Hoewel de governance van de functionaliteit volledig onder de verantwoordelijkheid van de onderwijsinstelling valt en deze functionaliteit zelf geen risico's met zich meebrengt, wordt het risico hier wel benoemd zodat onderwijsinstellingen zich bewust zijn van mogelijke aandachtspunten. Het is een redelijke mogelijkheid dat het een van de voornoemde risico's zich voordoet. Als een van de risico's zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene. Om die reden kwalificeert dit als een **hoog risico**.

16.1.8 Risico 8: Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd

In Recommendation 01/2020 van de EDPB geeft de EDPB aan dat encryptie een afdoende maatregel is tegen onbevoegde toegang indien het sleutelbeheer voldoet aan NIST 800-57. CACI voert echter geen audits volgens deze norm uit op het sleutelbeheer en kan daarmee niet aantonen dat de encryptie een afdoende beveiligingsmaatregel is.

De kans dat dit risico zich voordoet is redelijk, onder andere omdat het sleutelbeheer in Ansible mogelijkerwijs niet aan NIST 800-57 voldoet. De gevolgen voor de voor de rechten en vrijheden van de betrokkenen zijn enige negatieve gevolgen, omdat het onbevoegde toegang tot de back-ups makkelijker maakt. Dit kwalificeert als een medium risico.

16.1.9 Risico 9: Back-ups langer verwerkt dan nodig bij beëindigen contract

Bij het beëindigen van het contract met CACI, worden de accounts na 90 dagen inactief gemaakt en 90 dagen later de database gewist. Deze database blijft echter nog een jaar lang bewaard in de back-ups. Als CACI na het eindigen van de overeenkomst met de onderwijsinstelling de back-ups nog een jaar bewaard, worden deze gegevens langer verwerkt dan noodzakelijk. Hiermee wordt niet voldaan aan het beginsel van opslagbeperking.

Dit is de standaard werkwijze van CACI, dus als een onderwijsinstelling het contract met CACI beëindigt en niet expliciet teruggave of verwijdering verzoekt, dan zal dit risico zich voordoen (redelijke mogelijkheid). Niet voldoen aan het beginsel van opslagbeperking heeft ernstige gevolgen voor de rechten en vrijheden van de betrokkenen. Om die reden is dit een hoog risico voor de rechten en vrijheden van betrokkenen.

16.1.10 Risico 10: Onvoldoende transparantie over mobiele app

Dit is een risico dat algemeen geldt bij alle toepassingen waarbij een mobiele app wordt aangeboden via de AppStore of GooglePlay.

Er ontbreekt essentiële informatie over de verwerkingen met betrekking tot de mobiele app van Osiris: de verwerkte persoonsgegevens (device-ID, accountgegevens, naam onderwijsinstelling waar de student studeert) en de betrokken subverwerkers worden niet vermeld in de verwerkersovereenkomst. Hierdoor kan de onderwijsinstelling als verwerkingsverantwoordelijke betrokkenen niet op transparante wijze informeren over de gegevensverwerking. Zonder deze informatie kunnen betrokkenen geen weloverwogen keuzes maken over het gebruik van de dienst of de app, en kunnen zij hun rechten niet effectief uitoefenen.

De kans dat dit risico zich voordoet is redelijk. Hoewel instellingen zelf aanvullende informatie kunnen verzamelen over de verwerkingen binnen de mobiele app, is het mogelijk dat niet alle relevante informatie toegankelijk of toereikend is. Deze informatie dient CACI als ontwikkelaar proactief te verstrekken aan de onderwijsinstellingen. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkenen. Zij lopen het risico dat hun persoonsgegevens worden verwerkt zonder dat zij daar voldoende van op de hoogte zijn, wat kan leiden tot verlies van controle over hun gegevens. Om die reden kwalificeert dit als een **hoog risico**.

16.1.11 Risico 11: Mobiele app niet als 'side-load' beschikbaar

Dit is een risico dat algemeen geldt bij alle toepassingen waarbij een mobiele app wordt aangeboden via de Apple App Store of Google Play Store.

De mobiele app van Osiris is beschikbaar via de Apple App Store en de Google Play Store. Wanneer een student de app downloadt, ontstaat er automatisch een koppeling tussen het gebruik van de app en het persoonlijke Apple- of Google-account van de student. Deze platformen krijgen daardoor inzicht in het feit dat de app is geïnstalleerd, wat kan leiden tot indirecte identificatie van de onderwijsinstelling van de student. Deze vorm van gegevensverwerking is niet strikt noodzakelijk voor het aanbieden van de app, aangezien minder privacy-invasieve alternatieven bestaan. Bovendien levert het een verlies van controle over de persoonsgegevens op.

De kans dat het risico zich voordoet is waarschijnlijker dan niet, aangezien de mobiele apps van de instellingen niet als side-load beschikbaar zijn en gedownload moeten worden via de Apple App Store of the Google Play Store. De gevolgen voor de rechten en vrijheden van betrokkenen als dit risico zich voordoet zijn groot, aangezien gegevens van de student bij derde partijen terecht komen als gevolg van het gebruik van de mobiele app. Dit kwalificeert als een **hoog risico**.

16.1.12 Risico 12: Pushberichten veroorzaken verwerking door Google en Apple

Dit is een risico dat algemeen geldt bij alle toepassingen waarbij gebruik gemaakt wordt van de push infrastructuur van Google of van Apple.

De mobiele Osiris app verzendt pushberichten. De pushberichten veroorzaken zowel de overdracht van metadata en inhoud aan Google en Apple. De metadata betreft gegevens als device identifyers, IP-adressen en mogelijkerwijs het Google-account van de student. De inhoud betreft de berichten indien die inhoud onversleuteld verstuurd wordt, zoals noodzakelijkerwijs het geval is bij het 'notification messages' deel van de push berichten. De inhoud daarvan is zichtbaar voor en wordt verwerkt door Google. Onderwijsinstellingen bepalen zelf de inhoud van de berichten en kunnen daarin privacyvriendelijke keuzes maken, bijvoorbeeld door geen persoonsgegevens op te nemen. Ongeacht de inhoud van de berichten, wordt door het gebruik van notification messages de inhoud van de berichten structureel verwerkt door Google. Het is mogelijk om deze verwerking te reduceren door gebruik te maken van een encrypted data payload, al dan niet boven op de notification message. Indien een student Unified Push, een alternatieve push infrastructuur voor Android, beschikbaar heeft, dan kan de app daar ook gebruik van maken en terugvallen op Google als het niet beschikbaar is. Gezien de afwezigheid van beide mitigerende maatregelen, wordt met het gebruik van notification messages niet voldaan aan het subsidiariteitsvereiste.

De kans dat het risico zich voordoet is waarschijnlijker dan niet. De impact hangt af van de inhoud van de pushberichten. Indien deze persoonsgegevens bevat, heeft de verwerking mogelijk ernstige gevolgen voor de rechten en vrijheden van betrokkenen. Daarnaast wordt er bij notificaties metadata gedeeld met Google en Apple. In ieder geval heeft het gebruik van de push infrastructuur van Google en Apple enige negatieve gevolgen. Om die reden kwalificeert dit als een **hoog risico**.

16.1.13 Risico 13: Verwerkersovereenkomsten onvolledig m.b.t. mobiele app

De Osiris app maakt gebruik van Apple Push Notifications (APN) voor iOS en Firebase Cloud Messaging van Google voor Android. Deze diensten vereisen registratie van de mobiele telefoon met een apparaat-ID en API-key. Hoewel bij deze functionaliteit persoonsgegevens worden verwerkt, is de app (inclusief het gebruik van pushdiensten en de betrokken subverwerkers) niet opgenomen in de verwerkersovereenkomst met TiU. Hierdoor is onduidelijk welke subverwerkers betrokken zijn, welke persoonsgegevens zij verwerken en of er doorgifte plaatsvindt naar derde landen. Het is aannemelijk dat dit ook geldt voor de verwerkersovereenkomsten met andere onderwijsinstellingen.

Verwerkersovereenkomsten dienen volgens artikel 28 lid 3 AVG het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkings-verantwoordelijke te omschrijven. Doordat de mobiele app en de betrokken subverwerkers niet zijn opgenomen in de verwerkersovereenkomst, ontbreekt een expliciete instructie van de onderwijsinstelling aan CACI. Hierdoor ontstaat een verlies van controle over de verwerking van persoonsgegevens via de app.

De kans dat het risico zich voordoet is waarschijnlijker dan niet. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien er een verlies van controle is. Om die reden wordt dit risico gekwalificeerd als een **hoog risico**.

16.2 Beoordeling risico's

Door de aangetroffen risico's weer te geven op basis van hun potentiële impact op de rechten en vrijheden van de betrokkenen, ontstaat een beeld van de hoge en lage risico's die verbonden zijn aan de verwerking van persoonsgegevens in Osiris. In de risicografiek die door de Britse toezichthouder ICO is ontwikkeld, zien de risico's van het postproces er als volgt uit:

Tabel 26: Risico-overzicht

Ernst van de gevolgen voor de betrokkene(n)	Ernstige gevolgen	Laag risico	Hoog risico 1, 2, 4, 5, 6, 7, 9, 10	Hoog risico 3, 11, 12, 13
	Enige negatieve gevolgen	Laag risico	Medium Risico 8	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

Deel D: Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de verwerkingsverantwoordelijke.

17 Maatregelen

In dit onderdeel wordt beoordeeld welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Er wordt beschreven welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, wordt gemotiveerd waarom het restrisico acceptabel is.

17.1 Voorgestelde maatregelen

In deze DPIA zijn in totaal twaalf initiële hoge risico's en één medium risico voor de rechten en vrijheden van betrokkenen geïdentificeerd. Daarvan zijn vier hoge risico's gerelateerd aan de mobiele app. In dit deel worden per risico één of meer maatregelen voorgesteld om de initiële hoge risico's te mitigeren, zodat alleen lage restrisico's overblijven. Bij het bepalen van het restrisico gaat de DPIA ervan uit dat de instellingen de maatregelen aan hun kant implementeren.

Tabel 27: Voorgestelde maatregelen

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.	Restrisico
1.	Instellingen gebruiken Osiris als administratie studentpsycholoog.	Gebruik Osiris niet als administratie of dossier van de studentpsycholoog, totdat CACI de beschreven maatregel heeft getroffen.	Maak Osiris geschikt voor gegevens die onder de WGBO vallen.	Laag
2.	Instellingen verwerken mogelijk BSN bij digitaal ondertekenen met DigID zonder wettelijke grondslag.	Maak waar mogelijk gebruik van andere methoden voor ondertekenen.	Wijs instellingen op de mogelijk onrechtmatige verwerking.	Laag
		Beoordeel de grondslag voor het gebruik van de BSN indien ondertekenen met DigID geactiveerd is.		
3.	Bestandsnamen in applicatielogs.		Wijzig de configuratie van de applicatielogs zodat bestandsnamen niet meer worden opgenomen.	Laag
4.	Onvoldoende beoordeling van		Stel een procedure in om alle uitgegeven	Laag

	toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI).		toegangsrechten regelmatig te toetsen en te beoordelen aan de hand van de actuele autorisatiematrix.	
5.	Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens.	Neem zo weinig mogelijk bijzondere of gevoelige persoonsgegevens op in Osiris.	Optioneel: Bied de mogelijkheid aan om op veldniveau-encryptie toe te passen.	Laag
		Maak gebruik van de bestaande maatregelen, met name autorisatiemanagement, om de toegang tot bijzondere en gevoelige persoonsgegevens te beheren.		
6.	Onvoldoende governance koppelvlakken.	Richt de governance rond koppelvlakken adequaat in en controleer op naleving.		Laag
7.	Onvoldoende governance spiegeldatabase functionaliteit.	Indien gebruik gemaakt wordt van deze functionaliteit: richt adequate governance in om te voorkomen dat onbevoegde toegang of onrechtmatige verwerkingen ontstaan.		Laag
8.	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd.		Richt sleutelbeheer in conform NIST 800-57.	Laag
9.	Back-ups langer verwerkt dan nodig bij beëindigen contract.		Draag kopie database (via back-up) over aan instelling indien gewenst.	Laag

			Vernietig encryptiesleutel database (back-up) conform exitprocedure en verwerkers-overeenkomst.	
Risico's verbonden aan de mobiele app				
10.	Onvoldoende transparantie over mobiele app.	Gebruik de informatie die CACI levert om gebruikers van de mobiele app adequaat te informeren.	Lever volledige informatie over de gegevensverwerkingen in de mobiele app.	Laag
11.	Mobiele app niet als 'side-load' beschikbaar.	Voer proportionaliteits- en subsidiariteitsbeoordeling uit op beschikbaar stellen mobiele app als 'side-load' en implementeer resultaten.	Stel op verzoek van de instelling de application programme kit (APK) beschikbaar.	Laag
12.	Pushberichten veroorzaken verwerking door Google en Apple.	Configureer pushberichten zo dat deze geen persoonsgegevens bevatten.	Faciliteer dat pushberichten zonder persoonsgegevens ingericht kunnen worden.	Laag
			Pas de inrichting van de applicatie aan zodat Unified Push gebruikt kan worden, indien aanwezig op het apparaat van de gebruiker.	
13.	Verwerkersovereen komsten onvolledig m.b.t. mobiele app.	Vul de verwerkersovereenkomst aan met de verwerkingen die van toepassing zijn bij de mobiele app.	Vul de verwerkersovereen-komst aan met de verwerkingen die van toepassing zijn bij de mobiele app.	Laag

Conclusie

In deze DPIA zijn in totaal twaalf hoge risico's en één medium risico voor de rechten en vrijheden van betrokkenen geïdentificeerd. Daarvan zijn vier hoge risico's gerelateerd aan de mobiele app.

De risico's resulteren deels uit de wijze waarop instellingen Osiris gebruiken en deels uit de inrichting van Osiris zelf. Voor alle initiële hoge risico's zijn maatregelen voorgesteld. Elf van deze maatregelen gelden voor de instellingen en twaalf (plus een optionele maatregel) voor CACI.

Met het treffen van de maatregelen kunnen alle hoge risico's worden gemitigeerd, zodat alleen lage restrisico's overblijven. Er is dan geen voorafgaande raadpleging bij de Autoriteit Persoonsgegevens vereist.

CACI en SURF hebben afspraken gemaakt over hoe en wanneer CACI hun maatregelen gaat implementeren. De status hiervan is te vinden in Tabel 2: Overzicht status maatregelen. CACI is al begonnen met het implementeren van een deel van de maatregelen en alle maatregelen zullen binnen een acceptabele termijn geïmplementeerd worden. Daarom kan het gebruik van Osiris voorlopig worden voortgezet. In 2026 zal SURF een update over deze DPIA publiceren met een definitieve conclusie over de implementatie van de maatregelen.