

Bijlage risico's en maatregelen

12 september 2025

Onderstaande bijlage is overgenomen uit de Surf DPIA. Een uitgebreide toelichting op de risico's vindt u in de DPIA. In het groen hebben wij de laatste stand van zaken en/of vervolgstappen toegevoegd.

Er zijn totaal 13 risico's geïdentificeerd. Voor deze risico's moet CACI 12 maatregelen nemen, waarvan 3 optioneel zijn. De instellingen moeten 11 maatregelen nemen, en samen gaan we 2 maatregelen onderzoeken. CACI heeft al 5 maatregelen afgerond en is met de resterende 7 maatregelen al gestart, waarvan 3 de optionele maatregelen zijn. Tot nu toe zijn er 5 risico's volledig gemitigeerd, zodat er nog 8 risico's over zijn.

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
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. CACI: gestart. Met deze maatregel is reeds een begin gemaakt met een onderzoek naar de uitbreiding van de logging functionaliteit in Osiris. Samen met onze klanten zullen we de verdere aanpak vaststellen.
2.	Instellingen verwerken mogelijk BSN bij digitaal ondertekenen met DigiD zonder wettelijke grondslag. Gereed	Maak waar mogelijk gebruik van andere methoden voor ondertekenen.	Wijs instellingen op de mogelijk onrechtmatige verwerking. CACI: gereed. De 4 instellingen die gebruik maken van DigiD zijn geïnformeerd. Hiermee is de maatregel uitgevoerd. Op verzoek kunnen we samen met deze instellingen kijken naar de implementatie van een alternatieve ondertekening.
		Beoordeel de grondslag voor het gebruik van de BSN indien ondertekenen met DigiD geactiveerd is.	

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
3.	Bestandsnamen in applicatielogs. Gereed		Wijzig de configuratie van de applicatielogs zodat bestandsnamen niet meer worden opgenomen. CACI: gereed.
4.	Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI). Gereed		Stel een procedure in om alle uitgegeven toegangsrechten regelmatig te toetsen en te beoordelen aan de hand van de actuele autorisatiematrix. CACI: gereed. Wij passen de nieuwe beoordelingsmethode rond toegangsrechten inmiddels anderhalf jaar toe. Half augustus zijn de externe ISO 27001- en ISAE-audit uitgevoerd. Daarbij is geconstateerd dat de gehanteerde beoordelingsmethode effectief is.
5.	Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens.	Neem zo weinig mogelijk bijzondere of gevoelige persoonsgegevens op in Osiris. Maak gebruik van de bestaande maatregelen, met name autorisatiemanagement, om de toegang tot bijzondere en gevoelige persoonsgegevens te beheren.	Optioneel: Bied de mogelijkheid aan om op veldniveau-encryptie toe te passen. CACI: gestart. Ondanks dat dit voor CACI een optionele maatregel is, is CACI een onderzoek gestart naar technische mogelijkheden en consequenties.
6.	Onvoldoende governance koppelvlakken.	Richt de governance rond koppelvlakken adequaat in en controleer op naleving.	

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
		CACI: ondanks dat dit geen maatregel voor CACI is, ondersteunen we de instellingen op verzoek graag met een 'best practice'.	
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. CACI: ondanks dat dit geen maatregel voor CACI is, ondersteunen we de instellingen op verzoek graag met een 'best practice'. Opgemerkt wordt dat we standaard de mogelijkheid bieden om specifieke velden uit te sluiten voor de replicatie naar de spiegeldatabase.	
8.	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd.		Richt sleutelbeheer in conform NIST 800-57. CACI: gestart. Een onderzoek is gestart naar technische mogelijkheden en consequenties.
9.	Back-ups langer verwerkt dan nodig bij beëindigen contract. Gereed		Draag kopie database (via back-up) over aan instelling indien gewenst. CACI: gereed. Vernietig encryptiesleutel database (back-up) conform exitprocedure en verwerkers-overeenkomst. CACI: gereed.

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
			De exitprocedure is aangepast. De beschrijving van de procedure wordt opgenomen in de Standaard Dienstbeschrijving Osiris SaaS. Dit document wordt tweemaal per jaar geactualiseerd en gepubliceerd (mei en november). In november komt een geactualiseerde versie beschikbaar.

Risico's en maatregelen voor de Osiris Studenten App

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
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. CACI: gestart. CACI zal een addendum op de staande verwerkersovereenkomsten afstemmen met de betrokken klanten. Dit wordt voor eind 2025 afgerond. Voor nog af te sluiten verwerkersovereenkomsten zal dit nieuwe onderdeel standaard worden opgenomen.
11	Mobiele app niet als 'side-load' beschikbaar. Gereed	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. CACI: gereed.
12	Pushberichten veroorzaken verwerking door Google en Apple.	Configureer pushberichten zo dat deze geen persoonsgegevens bevatten.	Faciliteer dat pushberichten zonder persoonsgegevens ingericht kunnen worden. CACI: gestart.

#	Risico	Maatregel onderwijsinstelling	Maatregel CACI B.V.
			Inmiddels is onderzocht op welke manier de mogelijkheid om persoonsgegevens op te nemen in pushberichten geblokkeerd kan worden. CACI zal in overleg met de gebruikende instellingen deze maatregel binnen 6 tot 8 maanden doorvoeren. Pas de inrichting van de applicatie aan zodat Unified Push gebruikt kan worden, indien aanwezig op het apparaat van de gebruiker. CACI gestart. CACI doet onderzoek naar wat er nodig is om gebruikers in staat te stellen Unified Push te gebruiken voor de Osiris app, past de resultaten toe en de applicatie aan (uiterlijk Q2 2026).
13	Verwerkersovereenkomsten onvolledig m.b.t. mobiele app.	Vul de verwerkersovereenkomst aan met de verwerkingen die van toepassing zijn bij de mobiele app.	Vul de verwerkersovereenkomst aan met de verwerkingen die van toepassing zijn bij de mobiele app. CACI: gestart. CACI zal een addendum op de staande verwerkersovereenkomsten afstemmen met de betrokken klanten. Dit wordt voor eind 2025 afgerond. Voor nog af te sluiten verwerkersovereenkomsten zal dit nieuwe onderdeel standaard worden opgenomen.