Memo

Aan	SURF-leden
Van	SURF Vendor Compliance
Datum	13 april 2026
Kenmerk	Tussentijdse update
Betreft	Vervolgacties mbo naar aanleiding van DPIA Osiris

1. Introductie

In september 2025 heeft SURF Vendor Compliance een DPIA gepubliceerd over studenteninformatiesysteem Osiris van CACI B.V. De technische testscenario's voor deze DPIA zijn uitgevoerd in de testomgeving van Tilburg University. De DPIA heeft geresulteerd in twaalf hoge risico's en een medium risico voor gebruikers van Osiris. Zowel CACI als de onderwijsinstellingen zelf moeten maatregelen nemen om deze risico's te mitigeren. Als deze maatregelen worden genomen, kunnen instellingen het gebruik van Osiris voortzetten.

Na publicatie van de DPIA is SURF ter ore gekomen dat er onduidelijkheid en zorgen bestonden bij de mbo-sector over:

1. In hoeverre deze risico's op mbo-instellingen van toepassing zijn.
2. Welke maatregelen mbo-instellingen moeten nemen naar aanleiding van de DPIA.
3. Het ontbreken van bepaalde mbo-specifieke scenario's. Dit komt onder andere doordat er bij een universiteit is getest.

Vanwege deze onduidelijkheid bestaat het risico dat mbo's niet de benodigde maatregelen nemen, waardoor de gegevensbeschermingsrisico's voor hun gebruikers blijven bestaan. SURF Vendor Compliance zet daarom een extra stap door tijdens de update van de DPIA extra aandacht te geven aan de zorgen vanuit het mbo. In deze memo wordt uitgelegd hoe dat wordt gedaan.

2. Toepasselijkheid DPIA binnen het mbo

De risico's in de DPIA gelden in beginsel allemaal voor mbo-instellingen. Alleen als een scenario niet van toepassing is op een mbo-instelling, geldt het bijbehorende risico uit de DPIA niet voor die instelling. (Dit geldt ook voor hbo-instellingen en universiteiten, maar deze notitie is specifiek gericht op mbo-instellingen.) In onderstaande tabel laat de derde kolom zien onder welke voorwaarde een risico geldt voor een instelling, of dat het geldt voor alle instellingen. Als een risico geldt voor een instelling, moet die instelling alle

bijbehorende maatregelen nemen die de DPIA heeft vastgesteld. De vierde kolom laat zien of de DPIA maatregelen voor instellingen heeft vastgesteld.

Tabel 1 Toepasselijkheid risico's mbo-instellingen

Risico #	Risico	Toepasselijkheid	Maatregelen door instelling
1	Instellingen gebruiken Osiris als administratie studentpsycholoog.	Instellingen die studentpsychologen gebruiken	Ja
2	Instellingen verwerken mogelijk BSN bij digitaal ondertekenen met DigID zonder wettelijke grondslag.	Instellen die BSN's gebruiken bij het digitaal ondertekenen met DigID	Ja
3	Bestandsnamen in applicatielogs.	Alle instellingen	Nee
4	Onvoldoende beoordeling van toegangsrechten aan de hand van de autorisatiematrix (medewerkers CACI).	Alle instellingen	Nee
5	Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens.	Alle instellingen. Verwerken van gevoelige en bijzondere persoonsgegevens kan bijvoorbeeld voorkomen bij studieloopbaanbegeleiders.	Ja
6	Onvoldoende governance koppelvlakken.	Alle instellingen	Ja
7	Onvoldoende governance spiegeldatabase functionaliteit.	Instellingen die gebruik maken van spiegeldatabase functionaliteit	Ja
8	Sleutelbeheer van back-ups mogelijk niet voldoende beveiligd.	Alle instellingen	Nee
9	Back-ups langer verwerkt dan nodig bij beëindigen contract.	Alle instellingen	Nee
Risico's verbonden aan de mobiele app			
10	Onvoldoende transparantie over mobiele app.	Instellingen die de mobiele app gebruiken	Ja
11	Mobiele app niet als 'side-load' beschikbaar.	Instellingen die de mobiele app gebruiken	Ja
12	Pushberichten veroorzaken verwerking door Google en Apple.	Instellingen die de mobiele app gebruiken	Ja

13	Verwerkersovereenkomsten onvolledig m.b.t. mobiele app.	Instellingen die de mobiele app gebruiken	Ja

3. Missende testscenario's en verwerkingen

Om de DPIA uit te voeren heeft SURF tien testscenario's met acht verschillende rollen geformuleerd die bij het reguliere gebruik van Osiris voorkomen. De scenario's zijn uitgevoerd in de testomgeving van Tilburg University (TiU). Na publicatie van de DPIA bleek echter dat deze tien scenario's niet representatief waren voor al het reguliere gebruik van Osiris door mbo-instellingen.

Aanvullende testscenario's

Veel mbo-instellingen gebruiken de ouderportaalmodule van Osiris, waar TiU geen gebruik van maakt. Via dit portaal worden er gegevens verstrekt over mbo-studenten aan derdenontvangers, zoals ouders. Dit levert mogelijk verwerkingen met een hoog risico op en is dus relevant om mee te nemen in de testscenario's. Ook gebruiken veel mbo-instellingen de aanmeldmodule, module voor verzuimregistratie, intakemodule en module voor examinering. Daarnaast zijn er mbo-specifieke koppelingen die niet meegenomen zijn in de DPIA.

Aanvullende verwerkingen

Er worden bij mbo-instellingen andere typen bijzondere en gevoelige persoonsgegevens verwerkt dan bij hbo's en universiteiten door de verschillende behoeften van studenten. Dit gebeurt onder andere bij de studieloopbaanbegeleiders. Ook bij verwerkingen ten behoeve van beroepspraktijkvorming en verzuimregistratie worden deze typen gegevens verwerkt. Verder verwerken mbo-instellingen veel gegevens van minderjarigen, waar mogelijk aanvullende risico's voor gelden als kwetsbare groep.

4. Verduidelijking maatregelen

Ook bestaat er onduidelijkheid bij de mbo-instellingen over hoe om te gaan met de bestaande risico's en maatregelen uit de DPIA. Hieronder worden de meest relevante uitgelicht.

Risico 5: Verlies van vertrouwelijkheid bij bijzondere of gevoelige persoonsgegevens (onder andere door studieloopbaanbegeleiders)

Vanwege de reguliere doeleinden waar Osiris voor bestemd is, is het waarschijnlijk dat instellingen er bijzondere en/of gevoelige persoonsgegevens in verwerken, wat resulteert in een risico van verlies van vertrouwelijkheid. De eerste maatregel die de DPIA noemt is om dit soort gegevens zo min mogelijk in Osiris te verwerken. Met andere woorden, verwerk alleen bijzondere en/of gevoelige persoonsgegevens in Osiris als dit noodzakelijk is en er niet een geschikter systeem voor beschikbaar is. Bij mbo-instellingen gebeurt dit echter wel veel in het kader van de werkzaamheden van studieloopbaanbegeleiders. Door de aard van hun werkzaamheden hebben zij veel te maken met gevoelige informatie, ook over het persoonlijke leven van de student. De tweede maatregel die de DPIA dan ook noemt, is om de bestaande maatregelen die in Osiris beschikbaar zijn te gebruiken om de bijzondere/gevoelige persoonsgegevens die een instelling wel in Osiris verwerkt te

beheren. Op deze manier kan de instelling een gepast beveiligingsniveau bereiken en deze gegevens voldoende beschermen.

De DPIA gaat niet dieper in op deze bestaande maatregelen in Osiris en hoe die toe te passen. De maatregelen bestaan voornamelijk uit de juiste autorisaties configureren in Osiris, de juiste typen logging inschakelen en het inschakelen van veldencryptie voor velden waar bijzondere/gevoelige persoonsgegevens in staan, indien CACI dit mogelijk maakt.

Risico 6: Onvoldoende governance koppelvlakken
Risico 6 ontstaat als mbo-instellingen niet de juiste governance inrichten bij het gebruik van de koppelvlakkenfunctionaliteit. Met deze functionaliteit kan er gegevensuitwisseling met externe systemen plaatsvinden. Om onbevoegde toegang, datalekken of onrechtmatige gegevensverwerkingen te voorkomen, moeten instellingen gebruik maken van standaardfilters, SQL-queries, aangepaste eigen voorwaarden (“alleen tonen als …”), het uitsluiten van kolommen (zoals het BSN) en de bestaande permissies om te zorgen dat alleen de juiste gegevens worden gedeeld.

Risico 7: Onvoldoende governance spiegeldatabase
Risico 7 ontstaat als instellingen gebruik maken van de spiegeldatabasefunctionaliteit en daarbij niet de juiste governance inrichten. Met deze functionaliteit hebben instellingen de mogelijkheid om een (read only) replicatie van de database te maken en te exporteren naar een eigen server. Voor deze replicatie moeten door middel van goede governance dezelfde of vergelijkbare maatregelen gelden als voor de originele dataset, zodat instellingen disproportionele toegang, het niet naleven van bewaartermijnen, onrechtmatige verwerking, onvoldoende authenticatie of ongeoorloofde toegang tot bijzondere persoonsgegevens voorkomen.

Risico’s 10, 11, 12, 13: Risico’s verbonden aan de mobiele app
De DPIA identificeert vier risico’s en vier maatregelen voor instellingen die gebruik maken van de mobiele app. Eén van de maatregelen is een technische maatregel, namelijk om geen persoonsgegevens in pushberichten te verwerken. Twee maatregelen hebben te maken met het bieden van transparantie door de gegevensverwerkingen in de mobiele app zowel in de privacyverklaring als de verwerkersovereenkomst van de instelling op te nemen. CACI kan hier een ondersteunende rol bij spelen. De laatste maatregel is om een proportionaliteits- en subsidiariteitsbeoordeling uit te voeren op het beschikbaar stellen van de mobiele app via de app stores van Google en Apple of als “side load”. Anders gezegd betekent dit dat instellingen moet afwegen of het beschikbaar stellen van de app op een minder ingrijpende manier dan via deze twee app stores, die eigendom zijn van twee grote Amerikaanse big techpartijen. De DPIA biedt een aantal aanknopingspunten voor deze afweging, maar instellingen moeten de afweging maken voor hun individuele omstandigheden.

Geen risico: Bewaartermijnen
De DPIA heeft geen risico gevonden dat de inrichting van Osiris instellingen niet in staat stelt hun bewaartermijnen te handhaven. Osiris biedt de benodigde functionaliteiten zodat instellingen hun bewaartermijnen in Osiris kunnen inrichten. Dit betekent echter niet dat er geen actie is vereist van instellingen.

Om deze DPIA te kunnen gebruiken, moeten instellingen zorgen dat ze al hun verwerkingen in overeenstemming met de AVG vormgeven, ongeacht of er een risico aanwezig is bij het doen van die verwerkingen. Dit betekent (onder andere) dat instellingen zelf moeten zorgen dat elke verwerking een rechtsgrond, doeleinde, beveiligingsmaatregelen en ook een bewaartermijn heeft. Osiris biedt de mogelijkheden om bewaartermijnen te beheren, maar instellingen zijn zelf verantwoordelijk voor het vaststellen en handhaven van hun bewaartermijnen. Wel zal SURF onderzoeken of er voldoende documentatie is met uitleg over hoe instellingen de benodigde databasejobs/query's kunnen draaien om hun bewaartermijnen te handhaven.

5. Vervolgacties

Zowel mbo-instellingen als SURF moeten acties ondernemen naar aanleiding van de DPIA om te zorgen dat mbo-instellingen de risico's voor studenten, docenten en medewerkers kunnen mitigeren.

Mbo-instellingen

- ⇨ De verwerkingen van de instelling die plaatsvinden in Osiris in kaart brengen en in overeenstemming met de AVG inrichten.
- ⇨ Aan de hand van Tabel 1 Toepasselijkheid risico's mbo-instellingen identificeren welke risico's van toepassing zijn op de instelling.
- ⇨ De maatregelen die bij de risico's horen implementeren in de instelling en Osiris.

SURF

- ⇨ Extra toelichting op de maatregelen voor de instellingen opnemen in de update op de DPIA, in ieder geval:
  - Hoe het verlies van vertrouwelijkheid van bijzondere en gevoelige persoonsgegevens te mitigeren, onder andere door de juiste autorisaties te configureren in Osiris, de juiste typen logging in te schakelen, het handhaven van bewaartermijnen en het inschakelen van veldencryptie voor velden waar bijzondere/gevoelige persoonsgegevens in staan, indien CACI dit mogelijk maakt.
- ⇨ Aanvullende testscenario's zoals beschreven bij een mbo-instelling uitvoeren en de resultaten verwerken in de update op de DPIA:
  - Ouderportaal
  - Aanmeldmodule
  - Verzuimregistratie (AAR-module)
  - Intakemodule
  - Module voor examinering (Onderdeel Osiris Basis en Osiris Docent Begeleider)
  - Mbo-specifieke koppelingen

- ⇨ Aanvullende typen verwerkingen onderzoeken en evalueren, namelijk beroepspraktijkvorming, verzuimregistratie en studieloopbaanbegeleiding.
    - Studieloopbaanbegeleiding
    - Verzuimregistratie
    - Beroepspraktijkvorming
    - Verwerkingen van minderjarigen
    - Databasejob/query draaien om bewaartermijnen te handhaven

SURF verwacht bovenstaande aanvullingen en scenario's uit te werken in Q2 2026, waarna er in Q3 een volledige update op de DPIA gepubliceerd zal worden.

Voor meer informatie of vragen, neem contact op met: vendorcompliance@surf.nl.