Memo

To	SURF members
From	SURF Vendor Compliance
Date	13 april 2026
Reference	Interim update
Subject	Follow-up actions vocational colleges following the Osiris DPIA

1. Introduction

In September 2025, SURF Vendor Compliance published a DPIA on the Osiris student information system from CACI B.V. The technical test scenarios for this DPIA were carried out in Tilburg University's test environment. The DPIA identified twelve high risks and one medium risk for Osiris users. Both CACI and the educational institutions themselves must take measures to mitigate these risks. Provided these measures are taken, institutions may continue to use Osiris.

Following the publication of the DPIA, SURF became aware that there was uncertainty and concern within the vocational education sector regarding:

1. To what extent these risks apply to vocational colleges.
2. What measures vocational colleges must take in response to the DPIA.
3. The absence of certain scenarios specific to vocational colleges. This is partly because testing was carried out at a university.

Due to this uncertainty, there is a risk that vocational colleges will not take the necessary measures, meaning that data protection risks for their users will persist. SURF Vendor Compliance is therefore taking an extra step by paying particular attention to the concerns raised by the vocational education sector during the update of the DPIA. This memo explains how this will be done.

2. Applicability of the DPIA within vocational education

In principle, all the risks in the DPIA apply to vocational colleges. Only if a scenario does not apply to a vocational college does the corresponding risk from the DPIA not apply to that institution. (This also goes for universities of applied sciences and universities, but this memo focuses specifically on vocational colleges.) In the table below, the third column shows under what conditions a risk applies to an institution, or whether it applies to all institutions. If a risk applies to an institution, that institution must take all associated measures identified by the DPIA. The fourth column shows whether the DPIA has identified measures for institutions.

Table1 Applicability of risks to vocational colleges

Risk #	Risk	Applicability	Measures by institution
1	Institutions use Osiris for student psychologist administration.	Institutions that use student psychologists	Yes
2	Institutions may process BSNs when digitally signing with DigID without a legal basis.	Institutions that use BSNs when digitally signing with DigID	Yes
3	File names in application logs.	All institutions	No
4	Inadequate assessment of access rights based on the authorisation matrix (CACI staff).	All institutions	No
5	Loss of confidentiality regarding special or sensitive personal data.	All institutions. The processing of sensitive and special categories of personal data may, for example, occur in the case of study career counsellors.	Yes
6	Insufficient governance interfaces.	All institutions	Yes
7	Insufficient governance of mirror database functionality.	Institutions using mirror database functionality	Yes
8	Key management for backups may not be sufficiently secure.	All institutions	No
9	Backups are processed for longer than necessary upon termination of the contract.	All institutions	No
Risks associated with the mobile app			
10	Insufficient transparency regarding the mobile app.	Institutions using the mobile app	Yes
11	Mobile app not available as a ‘side-load’.	Institutions using the mobile app	Yes
12	Push notifications trigger processing by Google and Apple.	Institutions using the mobile app	Yes

13	Data processing agreements incomplete regarding the mobile app.	Institutions that use the mobile app	Yes

3. Missing test scenarios and data processing operations

To carry out the DPIA, SURF formulated ten test scenarios involving eight different roles that occur during the regular use of Osiris. The scenarios were carried out in the test environment at Tilburg University (TiU). However, following the publication of the DPIA, it became apparent that these ten scenarios were not representative of all regular use of Osiris by vocational colleges.

Additional test scenarios

Many vocational colleges use the Osiris parent portal module, which TiU does not use. Through this portal, data on vocational students is provided to third-party recipients, such as parents. This may involve high-risk processing and is therefore relevant to include in the test scenarios. Many vocational colleges also use the enrolment module, the absence registration module, the intake module and the examination module. In addition, there are data connectors specific to vocational colleges that have not been included in the DPIA.

Additional processing

Vocational colleges process different types of special and sensitive personal data compared to universities of applied sciences and universities, due to the differing needs of students. This occurs, for example, in the work of study career counsellors. These types of data are also processed in the context of vocational training and absence registration. Furthermore, vocational colleges process a significant amount of data relating to minors, which may entail additional risks as they constitute a vulnerable group.

4. Clarification of measures

There is also a lack of clarity among vocational colleges regarding how to deal with existing risks and measures from the DPIA. The most relevant of these are highlighted below.

Risk 5: Loss of confidentiality regarding special or sensitive personal data (including by study career counsellors)

Given the standard purposes for which Osiris is intended, it is likely that institutions process special and/or sensitive personal data within the application, resulting in a risk of loss of confidentiality. The first measure mentioned by the DPIA is to process this type of data in Osiris as little as possible. In other words, only process special and/or sensitive personal data in Osiris if this is necessary and there is not a more suitable system available. However, at vocational colleges, this does occur frequently in the context of the work carried out by study and career counsellors. Due to the nature of their work, they frequently deal with sensitive information, including details about students' personal lives. The second measure mentioned by the DPIA is therefore to use the existing controls available in Osiris to manage the special/sensitive personal data that an institution does

process in Osiris. In this way, the institution can achieve an appropriate level of security and adequately protect this data.

The DPIA does not go into further detail regarding these existing measures in Osiris and how to apply them. The measures mainly consist of configuring the correct authorisations in Osiris, enabling the correct types of logging, and enabling field encryption for fields containing special/sensitive personal data, where CACI permits this.

Risk 6: Inadequate governance of interfaces
Risk 6 arises if vocational colleges fail to establish the correct governance when using the interface functionality. This functionality enables data exchange with external systems. To prevent unauthorised access, data breaches or unlawful data processing, institutions must use standard filters, SQL queries, customised conditions ("show only if ..."), the exclusion of columns (such as the BSN) and existing permissions to ensure that only the correct data is shared.

Risk 7: Inadequate governance of the mirror database
Risk 7 arises when institutions use the mirror database functionality without implementing the correct governance. This functionality allows institutions to create a (read-only) replica of the database and export it to their own server. For this replication, good governance must ensure that the same or comparable measures apply as for the original dataset, so that institutions prevent disproportionate access, non-compliance with retention periods, unlawful processing, insufficient authentication or unauthorised access to special categories of personal data.

Risks 10, 11, 12, 13: Risks associated with the mobile app
The DPIA identifies four risks and four measures for organisations using the mobile app. One of the measures is a technical measure, namely not to process personal data in push notifications. Two measures relate to ensuring transparency by including the data processing activities in the mobile app in both the organisation's privacy statement and the data processing agreement. CACI can play a supporting role in this. The final measure is to carry out a proportionality and subsidiarity assessment regarding the availability of the mobile app via the Google and Apple app stores or as a 'side load'. In other words, this means that organisations must consider whether to make the app available in a less intrusive manner than via these two app stores, which are owned by two American big tech companies. The DPIA offers a number of starting points for this assessment, but organisations must make the assessment based on their individual circumstances.

No risk: Retention periods
The DPIA has not identified any risk that the design of Osiris prevents organisations from enforcing their retention periods. Osiris provides the necessary functionalities to enable organisations to configure their retention periods within Osiris. However, this does not mean that no action is required from organisations.

In order to use this DPIA, institutions must ensure that they structure all their processing operations in accordance with the GDPR, regardless of whether there is a risk associated with carrying out those operations. This means (among other things) that institutions themselves must ensure that every processing operation has a legal basis, a purpose, security measures and also a retention period. Osiris offers the ability to manage retention periods, but institutions are themselves responsible for determining and enforcing their retention periods. However, SURF will investigate whether there is sufficient documentation explaining how institutions can run the necessary database jobs/queries to enforce their retention periods.

5. Follow-up actions

Both vocational colleges and SURF must take action following the DPIA to ensure that vocational colleges can mitigate the risks to students, teachers and staff.

Vocational colleges

- ⇨ Map out the institution's processing activities that take place in Osiris and organise them in accordance with the GDPR.
- ⇨ UsingTable1 Applicability of risks to vocational colleges, identify which risks apply to the institution.
- ⇨ Implement the measures associated with the risks within the institution and in Osiris.

SURF

- ⇨ Include additional guidance on the measures for the institutions in the update to the DPIA, in any case:
  - How to mitigate the loss of confidentiality of special and sensitive personal data, including by configuring the correct authorisations in Osiris, enabling the correct types of logging, enforcing retention periods and enabling field encryption for fields containing special/sensitive personal data, if CACI allows this.
- ⇨ Carry out additional test scenarios as described for vocational colleges and incorporate the results into the update to the DPIA:
  - Parent portal
  - Registration module
  - Absence registration (AAR module)
  - Intake module
  - Examination module (Part of Osiris Basis and Osiris Docent Begeleider)
  - Connectors specific to vocational colleges
- ⇨ To investigate and evaluate additional types of data processing, namely work-based learning, absence recording and academic career guidance.
  - Study career guidance
  - Absence recording
  - Vocational training
  - Processing of data relating to minors
  - Running database jobs/queries to enforce retention periods

SURF expects to finalise the above additions and scenarios in Q2 2026, after which a full update to the DPIA will be published in Q3.

For further information or enquiries, please contact: vendorcompliance@surf.nl .