

# **Data Protection Impact Assessment on Qualtrics DesignXM**

## **SURF Vendor Compliance**

Dit is een vrijblijvende vertaling. Bij tegenstrijdigheden tussen deze vertaling en het originele document is het originele document leidend.

Auteurs: Valerija Kornilova, Julian Rill  
Versie: 1.0  
Datum: 17<sup>april</sup> 2026  
Contact: [vendorcompliance@surf.nl](mailto:vendorcompliance@surf.nl)  
DPIA door: <https://vendorcompliance.surf.nl/en>

Deze publicatie valt onder een Creative Commons  
Naamsvermelding 4.0 Internationaal.

## Samenvatting

Dit document is een DPIA (Data Protection Impact Assessment) met betrekking tot Qualtrics DesignXM. Deze DPIA is opgesteld in opdracht van SURF, de samenwerkingsorganisatie voor IT in het Nederlandse hoger onderwijs en onderzoek, ook wel afgekort als 'de Nederlandse onderwijssector' of 'onderwijsinstellingen'. Deze DPIA is een referentie-DPIA, wat betekent dat de bevindingen kunnen worden gebruikt door de SURF-leden en de onderwijssector.

### Over de dienst van Qualtrics

Qualtrics XM stelt organisaties in staat om realtime feedback te verzamelen van studenten, docenten en medewerkers via kanalen zoals enquêtes, online beoordelingen, interacties via callcenters en sociale media. Deze feedback biedt inzicht in de ervaringen en zorgen van de gemeenschap en ondersteunt initiatieven om de betrokkenheid van studenten te vergroten en het personeelsbehoud te verbeteren in een snel veranderend academisch landschap.

### Reikwijdte

Deze DPIA richt zich op het Qualtrics DesignXM-systeem. Binnen de aangeboden diensten aan de onderwijsinstellingen (SURF-leden) heeft SURF de reikwijdte bepaald op basis van de vragenlijst die in februari 2025 met onze onderwijsinstellingen is gedeeld.

Op basis van de vragenlijst die onder SURF-leden is verspreid, heeft SURF vastgesteld dat de digitale diensten van Qualtrics voornamelijk bedoeld zijn voor wetenschappelijk onderzoek in het onderwijs (toepassing van onderwijsmethoden), onderzoek (gegevensverzameling, gegevensverwerking en -analyse) en kennisbenutting (kennismarketing).<sup>1</sup> In het daaropvolgende onderzoek streefde SURF ernaar de reikwijdte van de institutionele activiteiten nauwkeurig te definiëren. Er werd vastgesteld dat Qualtrics DesignXM valt onder het domein Experience Management (XM).<sup>2</sup> Deze dienst kan worden gebruikt om de bedrijfsvoering van onderwijsinstellingen te verbeteren en de algehele ervaringen van studenten en medewerkers te optimaliseren. Het biedt tools voor beheerders, algemene gebruikers en onderzoekers om enquêtes te beheren, gegevens te verzamelen en analyses uit te voeren.

### Mogelijkheden voor algemene gebruikers en onderzoekers:

- Projecten aanmaken met behulp van sjablonen of aangepaste enquêtes
- Geavanceerde enquête-logica en validatiefuncties
- Kwaliteitscontroles van enquêtes via ExpertReview
- Samenwerkingsfuncties met aanpasbare machtigingen
- Meerdere distributiemethoden en het bijhouden van reacties
- Basisanalysetools en exportopties (SPSS, Excel, enz.)
- Instelling van quota voor representatieve steekproeven
- Ondersteuning voor vertalingen met automatische en handmatige opties

---

<sup>1</sup> De resultaten van de Qualtrics-enquête zijn op 15 februari met de aangesloten instellingen gedeeld.

<sup>2</sup> Qualtrics, 'Education Experience Management' (zonder datum) <https://www.qualtrics.com/education/> geraadpleegd op 17 maart 2026.

- Toegang tot trainingen, documentatie en ondersteuning via XM Basecamp en de Qualtrics Community

#### **Beheerdersfuncties (merkbeheerders):**

- Volledige controle over licenties, het aanmaken van gebruikers en machtigingsinstellingen
- Beheer van het privacybeleid (bijv. detectie van gevoelige gegevens, beveiligingsinstellingen)
- Toezicht op het gebruik van het platform (responspercentages, actieve gebruikers)

In deze DPIA wordt het doel van Qualtrics DesignXM als digitale dienst voor de instellingen nader toegelicht, evenals de functies die het biedt, aan de hand van een toelichting op de diensten, de verwerkte persoonsgegevens, de verwerkingsactiviteiten en de reacties op DSAR's (verzoeken om inzage van betrokkenen).

#### **Buiten het toepassingsgebied**

Deze DPIA heeft geen betrekking op diensten zoals Qualtrics CoreXM en Qualtrics AI Response. SURF voert tests uit binnen de omgeving van Qualtrics DesignXM.

#### **Uitslag van de DPIA**

Deze DPIA heeft 14 hoge en 1 laag risico geïdentificeerd die verband houden met het gebruik van Qualtrics DesignXM for Education. De door SURF in deel D voorgestelde risicobeperkende maatregelen bieden onderwijsinstellingen inzicht in de maatregelen die SURF heeft voorgesteld om een aantal van de risico's te beperken. Deze maatregelen hebben betrekking op lage risico's en functies die door de instellingen kunnen worden uitgeschakeld. Het is onwaarschijnlijk dat de hoge risico's kunnen worden opgelost zonder vaste en concrete toezeggingen van Qualtrics om passende technische en organisatorische maatregelen op leveranciersniveau te implementeren.

De vastgestelde hoge risico's hebben betrekking op het volgende: de gegevensagnostische aanpak, een onvolledige lijst van subverwerkers, verlies van controle en transparantie als gevolg van het onvolledig verzamelen van toestemming, onvolledige cookielijsten en een onvolledige afhandeling van de DSAR's. Maatregelen ter beperking van de risico's voor de onderwijsinstellingen zijn te vinden in deel D Beschrijving van voorgestelde risicobeperkende maatregelen. De leverancier heeft zich niet verbonden tot het implementeren van risicobeperkende maatregelen en heeft de risicoclassificatie van SURF betwist. Qualtrics heeft het afwijkende standpunt in de vorm van 'Oplegger' met SURF gedeeld; dit is opgenomen in de paragraaf Afwijkend standpunt van Qualtrics ('Oplegger')

#### **Error! Reference source not found.**

Het doel van SURF is ervoor te zorgen dat het gebruik van de producten van Qualtrics door klanten in het onderwijs in Nederland volledig in overeenstemming is met de AVG. SURF loopt voorop bij het uitvoeren en publiceren van de resultaten van DPIA's namens haar leden. Gezien de vastgestelde, nog niet opgeloste hoge risico's dringt SURF er bij onderwijsinstellingen op aan om de bevindingen van deze DPIA zorgvuldig in overweging te nemen alvorens het platform van Qualtrics te blijven gebruiken.

Mocht Qualtrics concrete toezeggingen doen om de nodige risicobeperkende maatregelen te implementeren, dan zal SURF deze beoordeling dienovereenkomstig bijwerken.

De onderstaande tabel geeft een overzicht van de resterende 14 hoge risico's en 1 laag risico.

| Nr. | Risico                                                                                                                                                | Door instellingen te nemen maatregelen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Door SURF aanbevolen maatregelen die Qualtrics moet nemen                                                                                                                                                                                                                                                                         |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Verlies van controle – Contractuele rolbepaling: Discrepancie tussen de juridische documentatie en de rol van de wederverkoper ( )                    | <p>Vermeld expliciet in de verwerkersovereenkomst dat meldingen van datalekken door de onderwijsinstellingen rechtstreeks aan de leverancier moeten worden gericht.</p> <p>SURF stelt voor om een rechtstreekse verwerkersovereenkomst met Qualtrics te ondertekenen.</p> <p>Indien een rechtstreekse verwerkersovereenkomst niet haalbaar of mogelijk is, voeg dan een addendum toe aan de huidige overeenkomst waarin wordt vastgelegd dat Qualtrics de enige verwerker is ( ) dient te worden aangeduid als 'reseller' of 'commerciële tussenpersoon'.</p> |                                                                                                                                                                                                                                                                                                                                   |
| 2   | Verlies van controle – Gegevensagnostische benadering: waardoor de rolverdeling tussen de partijen en het beginsel van doelbinding worden ondermijnd. | Aangezien de leverancier geen categorieën verstrekt, moet de instelling strikte 'datarecords' invoeren voor eindgebruikers zoals onderzoekers, medewerkers of studenten. Door te beperken welke velden op het platform kunnen worden aangemaakt, kan de instelling de categorieën van gegevens en betrokkenen 'zelf documenteren'.                                                                                                                                                                                                                            | <p>Modulaire openbare pagina met specifieke informatie over de gebruikelijke categorieën verwerkte gegevens en de doeleinden waaraan de persoonsgegevens zijn gekoppeld.</p> <p>Maak een duidelijk onderscheid tussen welke gegevens door Qualtrics als verwerkingsverantwoordelijke en/of gegevensverwerker worden verwerkt.</p> |

|   |                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                                                           | <p>Zorg ervoor dat alleen de 'geïnformeerde' kernverwerking plaatsvindt.</p> <p>Verbied het gebruik van het platform voor bijzondere categorieën gegevens.</p> <p>Onderwijsinstellingen moeten een expliciet verbod hebben op 'AI/LLM-training op basis van de verwerking van de gegevens van de klant'.</p> <p>Zorg ervoor dat in de eigen privacyverklaring van de onderwijsinstelling expliciet de categorieën persoonsgegevens worden vermeld die de leverancier verwerkt als gegevensverwerker en, eventueel, als verwerkingsverantwoordelijke. In Bijlage 1 moeten de categorieën persoonsgegevens worden gekoppeld aan de doeleinden.</p> | <p>Onderhandel met onderwijsinstellingen en neem in de verwerkersovereenkomst een expliciete bepaling op inzake 'Geen AI/LLM-training op basis van de verwerking van de gegevens van de klant'.</p> <p>Zich contractueel verbinden tot absolute anonimisering (niet alleen pseudonimisering) van alle gegevens die worden gebruikt voor 'Onderzoek en ontwikkeling' of 'Productverbetering'. Onderwijsinstellingen de mogelijkheid bieden om zich af te melden voor de anonimisatieprocessen.</p> <p>Breng de categorieën persoonsgegevens in kaart die Qualtrics verwerkt in overeenstemming met de 7 doeleinden waarvoor Qualtrics als verwerkingsverantwoordelijke optreedt</p> <p>Publiceer een openbare gegevensoverzicht voor alle Qualtrics-producten waarin elke mogelijke categorie van verzamelde persoonsgegevens wordt vermeld.</p> <p>Zorg voor een transparantiedashboard waarmee de beheerder kan zien welke categorieën precies worden gebruikt, bijvoorbeeld voor de ontwikkeling van diensten.</p> |
| 3 | Onvermogen om de rechten van betrokkenen uit te oefenen – | Wanneer in het DSAR-verzoek bepaalde categorieën gegevens ontbreken, moet er                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Qualtrics dient de ontbrekende loggegevens toe te voegen en het volledige                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|   |                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                               |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p>Transparantiekwestie met betrekking tot de DSAR-ondersteuning voor instellingen:</p> <p>Hoewel de antwoorden op enquêtes toegankelijk zijn, ontbreekt de loginformatie.</p>          | <p>binnen de instelling een formele procedure worden ingesteld waarbij een handmatig ticket naar de Qualtrics-helpdesk wordt gestuurd waarin specifiek om de ontbrekende gegevens wordt gevraagd.</p> <p>Geef de eindgebruikers uitleg over de vernieuwde DSAR-tool.</p>                                                                                                | <p>DSAR-antwoord aan onderwijsinstellingen te verstrekken.</p>                                                                                                                                                                                                                                                |
| 4 | <p>Gebrek aan transparantie in de lijst met subverwerkers – Onvolledige lijst met subverwerkers:</p> <p>De kern van dit risico is de niet openbaar gemaakte verwerking door derden.</p> | <p>Vraag de leverancier om de volledige lijst met subverwerkers en doe dit regelmatig binnen een onderwijsinstelling.</p> <p>Schakel de functies uit die verband houden met de verwerking door derden, totdat de leverancier een duidelijke beschrijving van het doel ervan toevoegt.</p>                                                                               | <p>Voeg de genoemde subverwerkers toe aan de lijst met subverwerkers.</p> <p>Bied een opt-out aan waarmee instellingen alle telemetrie door derden voor de eindgebruikers kunnen uitschakelen.</p>                                                                                                            |
| 5 | <p>Gebrek aan transparantierapporten:</p> <p>Het risico vloeit voort uit de informatieasymmetrie tussen de leverancier en het publiek.</p>                                              | <p>Hoewel het specifieke Qualtrics-rapport vertrouwelijk kan zijn, kan de instelling een algemene verklaring opnemen in haar eigen openbare transparantierapport.</p> <p>Bijvoorbeeld: <i>'Onze leveranciers hebben gemeld dat er in het afgelopen kalenderjaar geen verzoeken om gegevensopenbaarmaking zijn ontvangen van buitenlandse inlichtingendiensten.'</i></p> | <p>Lanceer een webpagina met geaggregeerde, geanonimiseerde statistieken over verzoeken van overheden wereldwijd. Deze moeten het volgende bevatten:</p> <p>Aantal ontvangen verzoeken;</p> <p>Het percentage verzoeken dat is aangevochten of afgewezen;</p> <p>Categorieën van de opgevraagde gegevens.</p> |
| 6 | <p>Gebrek aan transparantie – Inloggen via proxy</p> <p>Via proxy-aanmelding kunnen merkbeheerders toegang krijgen tot accounts van eindgebruikers zonder dat</p>                       | <p>Schakel inloggen via proxy uit.</p>                                                                                                                                                                                                                                                                                                                                  | <p>Implementeer realtime meldingen aan eindgebruikers. Dit moet bijvoorbeeld niet alleen zichtbaar zijn voor de beheerder, maar ook voor de gebruikers van wie de</p>                                                                                                                                         |

|   |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | deze hiervan op de hoogte worden gesteld.                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>identiteit wordt overgenomen.</p> <p>Op rollen gebaseerde beperkingen: beperk de toegang van een imitator tijdens een sessie.</p>                                                                                                                                                                                                                                                                                                                                                                       |
| 7 | Verlies van controle – interne systeem- en prestatielogboeken<br>Qualtrics legt technische statistieken en metagegevens vast in logbestanden die niet toegankelijk zijn voor de klant.                                                                        | Vermeld expliciet in de verwerkersovereenkomst dat prestatielogboeken deel uitmaken van de gegevenscategorie in Bijlage 1 van de verwerkersovereenkomst.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>Publiceer een lijst voor klanten waarin precies wordt vermeld welke metagegevens in prestatielogboeken worden vastgelegd.</p> <p>Verstrek een volledige kopie van de persoonsgegevens (inclusief het volledige DSAR).</p>                                                                                                                                                                                                                                                                               |
| 8 | Verlies van controle: heridentificatie van gepseudonimiseerde gegevens – anonimiserings technieken voor het trainen van AI-modellen<br>Het risico houdt verband met de 'black box'-benadering van de door de leverancier gebruikte anonimiserings technieken. | <p>Neem een strikte clause op in de verwerkersovereenkomst waarin staat dat anonimisering en aggregatie van institutionele gegevens voor AI-training of productverbetering strikt verboden zijn.</p> <p>Vraag formeel om een rapport over de statistieken voor de Nederlandse taal. Als de leverancier deze niet kan verstrekken, moet de instelling ervan uitgaan dat de anonimisering technisch ontoereikend is.</p> <p>Gebruik de instellingen van de merkbeheerder om alle generatieve AI-functies en geautomatiseerde inzichten globaal uit te schakelen totdat de leverancier een transparantiewitboek verstrekt met een lijst van alle gegevensvelden die worden geschoond.</p> | <p>Qualtrics moet een lijst publiceren van de gegevenstypen die zijn ML-model is getraind om te detecteren.</p> <p>Qualtrics moet transparanter zijn over de prestatie statistieken voor het Nederlands.</p> <p>Leg uit en toon het percentage/de statistieken van door AI geanonimiseerde gegevens die handmatig worden gecontroleerd door menselijke auditors.</p> <p>Wees transparanter over de Nederlandse prestatie statistieken; leg de drempels en meetwaarden uit voor de menselijke controle.</p> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                          |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9  | <p>Verlies van controle – Onvoldoende ondersteuning voor transparante communicatie met gebruikers en geïnformeerde toestemming</p> <p>De standaardcookiebanner van Qualtrics mist doorgaans een 'Alles weigeren'-knop op de eerste laag.</p>                                                                                                                                                                                | <p>Stel een speciaal toestemmingsformulier op.</p> <p>Geef onderzoekers de instructie om deze toestemmingsformulieren toe te voegen en in te voegen als er meta-informatie wordt gebruikt (naast andere '-vragen die mogelijk persoonsgegevens onthullen).</p>                                                                                                                | <p>Werk het algemene platformthema bij zodat een 'Alles weigeren'-knop standaard is opgenomen, in plaats van dat er aangepaste code van de klant nodig is.</p> <p>Herontwerp het toegangspunt van het platform zodat er geen niet-essentiële cookies (analytics, functionele voorkeuren) worden geplaatst totdat de toestemmings-API een positief signaal van de gebruiker ontvangt.</p> |
| 10 | <p>Verlies van controle – Toestemmingsbanner en locatiegegevens</p> <p>Geen toestemmingsbanner en het verzamelen van locatiegegevens.</p>                                                                                                                                                                                                                                                                                   | <p>Maak een speciaal toestemmingsformulier.</p> <p>Geef onderzoekers de opdracht om toestemmingsformulieren op te stellen en informeer de onderzoekers over de verwerking van locatiegegevens (naast andere vragen die mogelijk persoonsgegevens aan het licht brengen).</p>                                                                                                  | <p>Ontwerp de maatregel zodanig dat niet-essentiële cookies (analytics, functionele voorkeuren) worden uitgeschakeld totdat de toestemmings-API een positief signaal van de gebruiker ontvangt.</p>                                                                                                                                                                                      |
| 12 | <p>Verlies van controle – Onvolledige geautomatiseerde detectie door ExpertReview van specifieke gevoelige identificatiegegevens voor Nederlandse klanten in het onderwijs.</p> <p>De functie 'Beleid inzake gevoelige gegevens' beschikt niet over vooraf geconfigureerde 'onderwerpen' voor specifiek Nederlandse identificatiegegevens, waardoor deze functie zijn doel voor instellingen in Nederland niet vervult.</p> | <p>Stel het 'Beleid inzake gevoelige gegevens' zo in dat gevoelige informatie uit enquêtereacties wordt verborgen. Dit zorgt ervoor dat, zelfs als een respondent uit eigen beweging zijn BSN in een vrij tekstveld invoert, de gegevens worden vervangen door sterretjes of een andere vervangende tekenreeks.</p> <p>Configureer geen persoonsgegevens via ExpertReview</p> | <p>Verbeter Text iQ en ExpertReview zodat ze Nederlandse labels voor gevoelige gegevens herkennen. Het herkennen van bijvoorbeeld het BSN-nummer activeert dan waarschuwingen voor gevoelige gegevens.</p>                                                                                                                                                                               |

|    |                                                                                                                                                                                                                                                               |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                              |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | Gebrek aan transparantie – geen publicatie van nauwkeurigheidscijfers voor het beleid inzake gevoelige gegevens en het ontbreken van feedbackmechanismen<br>Het kernprobleem is het gebrek aan transparantie met betrekking tot de prestaties.                | Dien tickets of ondersteuningsverzoeken in bij Qualtrics voor de feedback.                                                                                                      | Qualtrics zou moeten deelnemen aan kwartaaloverleg om bekende detectiehiaten te bespreken en samen met SURF een stappenplan op te stellen voor het verbeteren van de identificatie van specifiek Nederlandse gegevens.<br><br>Voeg direct bij het beleid inzake gevoelige gegevens een knop ‘markeren als onnauwkeurig’ toe. |
| 14 | Verlies van controle – Automatisch gebruik van Google Translate en Amazon Translate<br>Ongecontroleerde gegevensstroom naar subverwerkers van die niet rechtstreeks worden beheerd door de beheerder van de instelling.                                       | De gebruiker die vertaalt, moet handmatig een actie uitvoeren (d.w.z. ‘AI vertaald naar EN’ toevoegen) in het veld.                                                             | Qualtrics zal een ingebouwde functie bieden waarmee de instelling de vertaaldiensten handmatig kan gebruiken.                                                                                                                                                                                                                |
| 15 | Overdracht buiten de EU/EER – Automatisch gebruik van Google Translate en Amazon Translate<br>Ongecontroleerde gegevensstroom naar subverwerkers die in de VS zijn gevestigd en niet rechtstreeks door de beheerder van de instelling worden beheerd.         | De eindgebruikers informeren over de vertaalfunctionaliteit.                                                                                                                    | Bied een andere optie voor vertaling aan: Europese alternatieven.<br><br>Bied beheerders de mogelijkheid om handmatig extra vertaalopties toe te voegen.                                                                                                                                                                     |
| 16 | Gebrek aan transparantie en ontbrekende toestemming als gevolg van onvolledige cookie-informatie<br>Zonder een volledige en nauwkeurige cookie-lijst is elke toestemming die van een student of onderzoeker wordt verkregen technisch ongeldig, aangezien zij | Geef de leverancier de formele opdracht om alle cookies die zijn aangemerkt als ‘Marketing’ of ‘Targeting’ en die niet strikt noodzakelijk zijn voor de dienst, te deactiveren. | Qualtrics moet een realtime, machinaal leesbare lijst verstrekken van alle cookies die momenteel in gebruik zijn. Dit zou onderwijsinstellingen in staat stellen hun eigen transparantieverklaringen automatisch bij te werken telkens wanneer de leverancier een nieuwe tracker toevoegt.                                   |

|  |                                                                                      |  |                                                                                                                                                                                                        |
|--|--------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | niet 'geïnformeerd' kunnen worden over tracking waarvan zij het bestaan niet kennen. |  | Voor elke gebruikte cookie moet Qualtrics een duidelijke technische motivering verstrekken waaruit blijkt dat deze 'strikt noodzakelijk' is in de zin van artikel 5, lid 3, van de e-privacyrichtlijn. |
|--|--------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Part C Beschrijving en beoordeling van risico's voor betrokkenen

Alvorens de details van de risicoclassificatie te onderzoeken, is het belangrijk te vermelden dat Qualtrics geen duidelijke uitleg heeft gegeven of de gestelde vragen voldoende heeft beantwoord. In deze DPIA is gekozen voor de 'black box'-benadering. Dit is de reden waarom sommige risico's als hoog zijn geclassificeerd, omdat er onvoldoende informatie van Qualtrics is verstrekt om een afgewogen DPIA uit te voeren. Het gebrek aan transparantie en medewerking van Qualtrics heeft het onderzoek belemmerd om tot een meer op samenwerking gebaseerd en goed onderbouwd resultaat te komen.

### C.1.1 Identificatie van risico's

Hieronder wordt een algemeen onderscheid gemaakt tussen de risico's van de verwerking van metagegevens enerzijds en de inhoudsgegevens anderzijds. Vervolgens worden 11 specifieke gegevensbeschermingsrisico's beschreven, waarvan er 7 betrekking hebben op de verwerking van diagnostische gegevens en 4 op de inhoudsgegevens. In het algemeen kunnen gegevensbeschermingsrisico's in de volgende categorieën voorkomen:

- - het onvermogen om rechten uit te oefenen (met inbegrip van, maar niet beperkt tot, privacyrechten);
  - het onvermogen om toegang te krijgen tot diensten of kansen;
  - verlies van controle over het gebruik van persoonsgegevens;
  - discriminatie;
  - identiteitsdiefstal of -fraude;
  - financieel verlies;
  - reputatieschade;
  - fysiek letsel;
  - verlies van vertrouwelijkheid;
  - heridentificatie van gepseudonimiseerde gegevens; of
  - enige andere significante economische of sociale nadelen<sup>3</sup>

### C.1.2 Classificatie van de risico's

Een risicomatrix wordt gebruikt om de factoren kans en impact visueel weer te geven en te classificeren. SURF maakt gebruik van de matrix van het Information Commissioner's Office ('ICO').<sup>4</sup>

---

<sup>3</sup> Information Commissioner's Office, *Overzicht van schade op het gebied van gegevensbescherming en de taxonomie van het ICO* (versie 1, april 2022) <https://ico.org.uk/media2/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf> geraadpleegd op 10 april 2026.

<sup>4</sup> Information Commissioner's Office, *Hoe voeren we een DPIA uit?* <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 10 april 2026.

De risicomatrix bestaat uit een tabel met twee assen, één aan de linkerkant en één aan de rechterkant, waarbij de kans op het optreden van een risico op de horizontale as staat en de impact op de verticale as.

|                                  |                 |             |                  |                           |
|----------------------------------|-----------------|-------------|------------------|---------------------------|
| Ernst van de impact              | Ernstige impact | Laag risico | Hoog risico      | Hoog risico               |
|                                  | Enige impact    | Laag risico | Gemiddeld risico | Hoog risico               |
|                                  | Minimale impact | Laag risico | Laag risico      | Laag risico               |
|                                  |                 | Heel klein  | Redelijke kans   | Waarschijnlijker dan niet |
| Waarschijnlijkheid/kans opschade |                 |             |                  |                           |

Figuur1 Risicomatrix

## C.2 Risico's voor betrokkenen

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. Dit deel begint met een algemene inventarisatie van de risico's voor de rechten en vrijheden van betrokkenen als gevolg van de verwerking van de persoonsgegevens en metagegevens van de klant (inclusief de doeleinden van de verwerking van de betreffende persoonsgegevens). De risico's worden vervolgens ingedeeld op basis van de waarschijnlijkheid dat ze zich voordoen en de impact op de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen.

### C.2.1 Verlies van controle – Bepaling van de contractuele rol (Laag)

De gegevensverwerkingsovereenkomst (verwerkersovereenkomst) met onderwijsinstellingen via een wederverkoper, [REDACTED] is geen verwerkersovereenkomst die is gesloten tussen een onderwijsinstelling en Qualtrics, maar via een wederverkoper. In de verwerkersovereenkomst is vastgelegd dat zowel de leverancier als de wederverkoper verwerkers zijn. Dit leidt tot onduidelijkheid over de rolverdeling en vergroot het risico op misverstanden over de verantwoordelijkheden die Qualtrics en [REDACTED] als verwerkers hebben. [REDACTED] kan echter geen verwerker zijn, omdat [REDACTED] geen platformleverancier is, maar een wederverkoper. De grondslag voor dit risico is toegelicht in het gedeelte over **Error! Reference source not found.**

De onduidelijkheid over de rolverdeling vergroot de kans op onrechtmatige verwerking vanwege een mogelijk gebrek aan duidelijke verantwoordelijkheden. Het is niet redelijk om te vermelden dat zowel de leverancier als de wederverkoper verwerkers zijn, en dit belemmert de rechtstreekse contractuele band tussen de feitelijke verwerker (Qualtrics) en de verwerkingsverantwoordelijke (onderwijsinstellingen). Als de onderwijsinstelling bijvoorbeeld een AVG-gerelateerd verzoek rechtstreeks bij Qualtrics indient, zou de veronderstelling (voortkomend uit de verwerkersovereenkomst) kunnen zijn dat dergelijke informatie ook door de wederverkoper kan worden verstrekt. In de praktijk beschikt de wederverkoper echter niet over deze informatie. Deze discrepantie tussen contractuele rechten en de operationele realiteit vloeit voort uit de lacunes in de documentatie, waarbij de wederverkoper ten onrechte als verwerker wordt aangemerkt. Daarom is de impact groot.

De kans op operationele tekortkomingen is heel klein, omdat het aantal instellingen gering is en onderwijsinstellingen de rol van de wederverkoper ████████ in de verwerkersovereenkomst kunnen aanpassen. Anders zouden verwerkingsverantwoordelijken ten onrechte kunnen aannemen dat zij op de wederverkoper kunnen vertrouwen om AVG-rechten, zoals verzoeken van betrokkenen, af te dwingen vanwege een indirecte contractuele band.

Het risico van een onduidelijke rolbepaling is daarom laag. Onderwijsinstellingen moeten ofwel bestaande overeenkomsten aanpassen en vermelden dat alleen Qualtrics een verwerker is, ofwel een directe contractuele overeenkomst sluiten om dit risico voor de betrokkenen te beperken.

### **C.2.2 Verlies van controle – een gegevensagnostische aanpak die de rolverdeling tussen de partijen en het beginsel van doelbinding ondermijnt (Hoog)**

Er zijn lacunes in de documentatie geconstateerd tijdens de beoordeling van de documentatie met betrekking tot de Qualtrics XM-diensten. In het begin van het DPIA-proces weigerde Qualtrics meer informatie te delen dan wat openbaar beschikbaar was of via het Trust Centre, wat onvoldoende was om de lacunes in de ontbrekende informatie of onvolledige documentatie in openbare documenten zoals het privacybeleid, de algemene voorwaarden en de door onderwijsinstellingen opgevraagde documentatie, zoals de verwerkersovereenkomst, op te vullen.

Daarnaast vermeldde SURF in het gedeelte over **Error! Reference source not found.** dat Qualtrics volgens deze 7 doeleinden optreedt als verwerkingsverantwoordelijke (volgens het privacybeleid):

- 1) Het leveren van de diensten;
- 2) Om met de klant te communiceren over de diensten;
- 3) Om de diensten te verbeteren, te monitoren, te personaliseren en te beveiligen;
- 4) Voor onderzoek en ontwikkeling;
- 5) Voor marketing en reclame;
- 6) Voor naleving en bescherming;
- 7) Om kunstmatige-intelligentietools te trainen.

Qualtrics treedt zowel op als verwerker (namens instellingen) als verwerkingsverantwoordelijke (voor eigen doeleinden, zoals analyse en AI-training). Qualtrics verwerkt echter ook persoonsgegevens die onder de verwerkersovereenkomst vallen voor eigen doeleinden, zoals de ontwikkeling van diensten, waaronder het trainen van LLM's. Ongeautoriseerde verwerking van persoonsgegevens voor eigen doeleinden van de leverancier kan grote gevolgen hebben voor de betrokkenen. Als Qualtrics de persoonsgegevens zonder rechtsgrondslag hergebruikt voor eigen doeleinden, is dit in strijd met het beginsel van doelbinding. SURF heeft vastgesteld dat persoonsgegevens mogelijk worden gebruikt om AI-tools te trainen.<sup>5</sup> Om te controleren of de doeleinden overeenkomen met de doeleinden die in de verwerkersovereenkomst en andere overeenkomsten zijn vastgelegd, moet in bijlage 1 van de verwerkersovereenkomst een lijst worden opgenomen van persoonsgegevens en categorieën persoonsgegevens die bij het

---

<sup>5</sup> <https://www.qualtrics.com/privacy-statement/>

betreffende doel horen, zodat een duidelijk en transparant overzicht van de gegevensverwerkingsactiviteiten wordt geboden.

In dergelijke opzetten is de categorisering van gegevens vaak vaag of onvolledig, vooral wanneer deze niet duidelijk is gescheiden in contracten of privacyverklaringen. Qualtrics heeft de soorten persoonsgegevens (de subset van klantgegevens) verstrekt die doorgaans door de klant worden gedefinieerd. Deze gegevens werden opgenomen in de tabel '**Error! Reference source not found.**'. Tijdens het technisch onderzoek constateerde SURF dat Qualtrics de gegevens verder verwerkt voor ontwikkelingsdoeleinden wanneer persoonsgegevens zijn geanonimiseerd en geaggregeerd. Qualtrics verklaart dat het een duidelijke scheiding handhaaft tussen zijn rollen als verwerker en verwerkingsverantwoordelijke.<sup>6</sup>

De kans op schade is groot, omdat er aan SURF geen informatie wordt verstrekt over de verwerkingsdoeleinden, de rechtsgrondslagen voor de verwerking, de categorieën gegevens en betrokkenen, en de criteria voor het bewaren van gegevens. Zonder deze duidelijkheid over het specifieke en rechtmatige doel, en bij ontoereikende documentatie, is het risico groot dat er bij niet-naleving geen duidelijk en volledig verwerkingsdocument kan worden overgelegd.

SURF beseft dat de leverancier een gegevensagnostische aanpak hanteert en handelt in opdracht van de onderwijsinstellingen (zijn klanten). Zonder de doeleinden te koppelen aan de categorieën persoonsgegevens in bijlage 1 van de verwerkersovereenkomst is het voor onderwijsinstellingen echter moeilijker om te controleren of hun interne doeleinden in overeenstemming zijn met de contractueel overeengekomen doeleinden. Dit vergroot de kans dat gegevens worden verwerkt op een manier die niet in overeenstemming is met de overeenkomsten met onderwijsinstellingen.

De impact in deze situatie is ernstig, omdat er sprake is van niet-naleving van de kernbeginselen van de AVG volgens artikel 5, lid 1, van de AVG. Hoewel SURF de beschikbare categorieën persoonsgegevens die door Qualtrics in de rol van verwerkingsverantwoordelijke worden verwerkt, heeft gecategoriseerd (zie**Error! Reference source not found.**), heeft Qualtrics geen volledig overzicht verstrekt van de persoonsgegevens die namens de klanten worden verwerkt. Het onvermogen om aan te tonen dat Qualtrics voldoet aan de kernbeginselen van de AVG kan daarom het vertrouwen binnen onderwijsinstellingen ondermijnen en de grondrechten van betrokkenen aantasten.

### **C.2.3 Onvermogen om de rechten van betrokkenen uit te oefenen – Transparantiekwestie met betrekking tot de ondersteuning van instellingen bij verzoeken om inzage (DSAR). (Hoog)**

Volgens de AVG-vereisten moeten betrokkenen worden geïnformeerd over de categorieën verzamelde persoonsgegevens, de doeleinden en de bewaartermijnen. Als er onvoldoende ondersteuning is voor onderwijsinstellingen, kan een leverancier het recht op toegang tot gegevens belemmeren (artikelen 13 en 14 AVG).

---

<sup>6</sup> Antwoord van Qualtrics aan SURF van 9 december 2025.

In de beginfase van ons technisch onderzoek constateerde SURF dat de toegang tot persoonsgegevens via de gebruikersinterface van het platform beperkt is tot gegevens uit enquêtereacties, met uitsluiting van cruciale, door het systeem gegenereerde gegevens, metagegevens van gebruikersaccounts, foutenlogboeken of toegangsgegevens. Bovendien weigert de leverancier rechtstreeks te helpen bij verzoeken om inzage in gegevens (DSAR's) voor gegevens die namens de instelling worden verwerkt, en verwijst hij gebruikers in plaats daarvan naar een algemene zelfhulppagina. Deze pagina behandelt alleen het handmatig exporteren van enquêtegegevens van respondenten en biedt geen ondersteuning voor het verkrijgen van toegang tot bredere persoonsgegevens die door het systeem worden verwerkt.

Qualtrics beschrijft deze aanpak vanwege de verantwoordelijkheid van de verwerkingsverantwoordelijke om zijn betrokkenen de DSAR te verstrekken:

*'Verantwoordelijkheid van de verwerkingsverantwoordelijke voor DSAR's: Op grond van de verwerkersovereenkomst is Qualtrics, indien het een verzoek van een betrokkene met betrekking tot persoonsgegevens ontvangt, verplicht de klant hiervan onmiddellijk op de hoogte te stellen en zal Qualtrics niet zelf op het verzoek reageren. In plaats daarvan vraagt Qualtrics de betrokkene het verzoek door te sturen naar de klant. Dit komt doordat de klant, als verwerkingsverantwoordelijke, de directe relatie met de betrokkenen heeft en als enige de doeleinden en middelen van de verwerking bepaalt.'*<sup>7</sup>

Daarom is het de verantwoordelijkheid van de klant om het volledige antwoord op het DSAR te verstrekken. Dit sluit aan bij de keuze van de leverancier om een gegevensagnostisch platform te zijn. Betrokkenen hebben echter het recht om een 'kopie' van persoonsgegevens te verkrijgen, wat betekent dat de betrokkene een getrouwe en begrijpelijke weergave van al die gegevens moet krijgen.<sup>8</sup>

Qualtrics maakt gebruik van een DSAR-tool die wordt beschreven in de sectie **Error! Reference source not found.** . Deze nieuwe DSAR-exporttool vult de aanvankelijk ontbrekende informatie aan, maar de loggegevens ontbreken nog steeds.

De impact van het verstrekken van onvoldoende informatie aan klanten ten aanzien van betrokkenen is groot, omdat de grondrechten van de betrokkenen van de klanten op het spel staan. Qualtrics heeft in het begin geen volledige informatie verstrekt, en onderwijsinstellingen konden daardoor evenmin voldoen aan hun verplichting als verwerkingsverantwoordelijke om een betrokkene volledige informatie te verstrekken.

De kans dat het risico zich voordoet is waarschijnlijk groter dan niet, omdat de waarschijnlijkheid dat betrokkenen een DSAR ontvangen waarin de loggegevens ontbreken, of onvolledige informatie over gegevensverwerking zoals de door Qualtrics gebruikte anonimiseringstechnieken en LLM-training, ertoe leidt dat de rechten van de betrokkenen niet door hen kunnen worden uitgeoefend.

---

<sup>7</sup> Antwoord van Qualtrics op de vraag van SURF van 9 december 2025.

<sup>8</sup> Zaak C-487/21, Österreichische Datenschutzbehörde en CRIF.

Over het geheel genomen is het risico hoog.

#### **C.2.4 Gebrek aan transparantie in de lijst van subverwerkers – Onvolledige lijst van subverwerkers (Hoog)**

Tijdens het technisch onderzoek werden enkele aanvullende diensten ontdekt, zoals Google Analytics (Google LLC), Pendo en Amplitude. Deze subverwerkers waren ofwel onvolledig beschreven, ofwel ontbraken ze volledig op de officiële lijst van subverwerkers. Aangezien Qualtrics onvoldoende informatie verstrekt over zijn gegevensverwerkingsactiviteiten – die door de leverancier als vertrouwelijk worden beschouwd – leidt het onvermogen om gebruikers te informeren over de daadwerkelijke verwerking van persoonsgegevens door derden tot juridische en operationele risico's voor onderwijsinstellingen. SURF heeft in het hoofdstuk **'Error! Reference source not found.'** bewijs geleverd dat er meer partijen bij de gegevensverwerkingsactiviteiten betrokken zijn dan in de lijst met

De impact is ernstig omdat verwerkers volgens de AVG de verwerkingsverantwoordelijken moeten informeren over derde verwerkers die bij de gegevensverwerking betrokken zijn. Qualtrics informeert gebruikers weliswaar over nieuwe subverwerkers door de e-mailmelding met klanten te delen, maar deze worden niet vermeld in de lijst met subverwerkers. De kans op schade is waarschijnlijker dan niet omdat uit eindpuntonderzoek tijdens het gebruik van het platform bleek dat er regelmatig verbindingen werden gemaakt met domeinen die verband houden met Google Analytics, Pendo en Amplitude, die allemaal niet op transparante wijze worden vermeld in de officiële documentatie van de leverancier over subverwerkers. Daarom is het risico hoog.

#### **C.2.5 Gebrek aan transparantie voor de optionele subverwerker Imperium LLC (geen risico meer)**

Qualtrics kan Imperium, LLC, een in de VS gevestigde optionele subverwerker, inschakelen om apparaatvingerafdrukken te maken en fraude op te sporen door het verzamelen van metadata zoals IP-adressen, browser-/apparaatinformatie en scores voor botdetectie. Dit houdt profilering en subverwerkers van Qualtrics is opgenomen.<sup>9</sup> Het maken van vingerafdrukken in. Het is echter onduidelijk wanneer en hoe Imperium daadwerkelijk wordt geactiveerd, aangezien merkbeheerders of onderzoekers geen inzicht krijgen in het gebruik ervan bij specifieke reacties. Ook is er geen duidelijk controlespoor of logboek dat bevestigt of metadata door Imperium wordt verwerkt.

Dit leidt tot een gebrek aan transparantie en verantwoording bij de verwerking van persoonsgegevens via derden.

Volgens overweging 30 van de AVG mogen metagegevens zoals apparaatkenmerken, IP-adressen en browsersignaturen worden gebruikt voor fingerprinting en worden deze beschouwd als persoonsgegevens. Dit soort profilering kan: inbreuk maken op de privacyrechten van gebruikers, in sommige rechtsgebieden de noodzaak van uitdrukkelijke toestemming met zich meebrengen (met name onder de e-privacyverordening en voor cookie-achtige technologieën),

---

<sup>9</sup> Qualtrics, 'Lijst van subverwerkers' (Qualtrics, z.j.) <https://www.qualtrics.com/subprocessor-list/> geraadpleegd op 14 april 2026.

en gedetailleerde transparantie in het privacybeleid vereisen. Daarom kunnen de gevolgen voor betrokkenen nadelig zijn, aangezien Qualtrics online identificatiegegevens gebruikt.

Er is een redelijke kans dat, hoewel Imperium LLC als ‘optioneel’ wordt aangemerkt, het ontbreken van een duidelijk opt-in- of opt-out-mechanisme een situatie creëert waarin de verwerking standaard actief is of indirect in gang wordt gezet. Daarom is het waarschijnlijk dat deze subverwerker onder bepaalde omstandigheden wordt ingeschakeld zonder dat de verwerkingsverantwoordelijke of de gebruiker zich daarvan bewust is.

Gezien de impact en de waarschijnlijkheid dat dit risico zich voordoet, werd het als hoog ingeschaald.

Aangezien Qualtrics echter is gestopt met het gebruik van Imperium LLC, is dit risico niet langer van toepassing op deze DPIA. Daarnaast wordt Qualtrics geadviseerd deze subverwerker uit de lijst van subverwerkers te verwijderen.<sup>10</sup>

### **C.2.6 Gebrek aan transparantie – transparantierapport (Hoog)**

Qualtrics publiceert geen transparantierapporten over verzoeken van overheidsinstanties. Qualtrics heeft verklaard dat het geen transparantierapporten over verzoeken van overheidsinstanties openbaar maakt. Bovendien staat in de gegevensverwerkingsovereenkomst (verwerkersovereenkomst) vermeld dat Qualtrics persoonsgegevens mag verwerken indien dit op grond van toepasselijke wetgeving vereist is en dat Qualtrics de klant op de hoogte stelt van die wettelijke verplichting. Deze aanpak mist echter transparantie met betrekking tot het aantal verzoeken van overheidsinstanties dat Qualtrics ontvangt, met name wat betreft de frequentie van verzoeken om gegevens door overheidsinstanties, de soorten verzoeken (nationale veiligheid, wetshandhaving), of verzoeken zijn ingewilligd of afgewezen, en of er gegevens van EU-burgers bij betrokken waren. Volgens de artikelen 13 en 14 van de AVG moeten de verwerkingsverantwoordelijken (onderwijsinstellingen) de betrokkenen informatie verstrekken over de persoonsgegevens die van hen zijn verzameld.

Tussenhandeldiensten (waaronder onlineplatforms) zijn krachtens de Wet op digitale diensten (‘DSA’) verplicht om transparantierapporten te verstrekken over hun activiteiten op het gebied van inhoudsmoderatie.<sup>11</sup> Deze verplichting omvat het verstrekken van jaarlijkse rapportages die openbaar en gemakkelijk toegankelijk zijn. De informatie moet onder meer betrekking hebben op overheidsbevelen, zoals het aantal bevelen dat van overheidsinstanties is ontvangen. De DSA legt meer specifieke verplichtingen op en weerspiegelt het erkende risico van een informatiekloof tussen het platform en de betrokkenen.

Het standpunt en de contractuele verplichtingen van Qualtrics zijn:

*‘• SCC-specifiek rapport: Qualtrics zal de klant jaarlijks een rapport ter beschikking stellen met statistische informatie over verzoeken van inlichtingendiensten tot openbaarmaking van persoonsgegevens die zijn overgedragen op basis van de standaardcontractbepalingen (SCC’s).*

---

<sup>10</sup> Qualtrics, ‘Lijst van subverwerkers’ (Qualtrics, z.d.) <https://www.qualtrics.com/subprocessor-list/> geraadpleegd op 14 april 2026.

<sup>11</sup> Artikel 15 van de Wet op digitale diensten („DSA“)

- *Inhoud van het rapport: Dit specifieke rapport vermeldt het aantal van dergelijke verzoeken dat in een bepaald kalenderjaar is ontvangen.*<sup>12</sup>

Ondanks het verstrekken van het rapport aan de klanten leidt het gebrek aan transparantie voor de betrokkenen tot een informatiekloof voor hen. Dit heeft grote gevolgen voor de betrokkenen. De betrokkenen zouden het rapport moeten ontvangen, omdat eindgebruikers deze informatie openbaar zouden moeten kunnen ontvangen, en niet alleen zodat de leverancier een *‘nalevingsmechanisme voor de contracterende klant kan bieden om diens toezicht in het kader van internationale vereisten voor gegevensoverdracht te vergemakkelijken*’<sup>13</sup>, wat niet bijdraagt aan een beter transparantiemechanisme om de betrokkenen te informeren over de verzoeken van de overheid.

De kans dat het risico zich voordoet is waarschijnlijker dan niet, omdat de mogelijkheid bestaat dat betrokkenen niet op de hoogte worden gebracht. Vanuit het perspectief van de verantwoordingsplicht van de verwerker heeft Qualtrics dit mechanisme ontworpen om te voldoen aan zijn eigen contractuele en wettelijke verplichtingen jegens de klanten, en niet jegens de betrokkenen. Daarom moeten onderwijsinstellingen, als verwerkingsverantwoordelijken, de betrokkenen proactief informeren via privacyverklaringen en transparantierapporten op basis van het SCC-specifieke rapport van Qualtrics. In de praktijk verwijzen onderwijsinstellingen naar de openbaar beschikbare informatie van Qualtrics. Dit sluit de details uit over de informatie die van de betrokkenen is verzameld, omdat Qualtrics deze uitsluitend met de klanten deelt.

Het gebrek aan transparantie (met betrekking tot met wie, wanneer en waarom de informatie van de betrokkenen met overheidsinstanties is gedeeld) en het effect op de verwerking van persoonsgegevens hebben een ernstige impact op de betrokkenen. Er moet duidelijk worden gecommuniceerd hoe de verwerkingsverantwoordelijken en de verwerker (om de verwerkingsverantwoordelijke te ondersteunen bij het delen van deze informatie met de betrokkenen) deze details aan de betrokkenen verstrekken. De waarschijnlijkheid dat het risico zich voordoet voor de betrokkene is aanzienlijk, omdat de kans dat betrokkenen niet worden geïnformeerd groot blijft. Onderwijsinstellingen kunnen de kans op deze risico’s verkleinen door deze informatie aan de betrokkene te verstrekken. Dit risico wordt als hoog ingeschat.

### **C.2.7 Gebrek aan transparantie – Inloggen via proxy (Hoog)**

Deze functie wordt beschreven in de sectie **Error! Reference source not found.** . De eindgebruiker ontvangt geen melding dat er een proxy-aanmelding heeft plaatsgevonden. De proxy-functionaliteit voldoet op twee manieren niet aan de transparantieplicht van de AVG: op het moment van toegang (de eindgebruiker weet niet dat er in realtime toegang tot zijn account wordt verkregen) en achteraf (geen meldingsmechanisme).

De impact op de betrokkenen is ernstig, omdat de eindgebruiker er geen weet van heeft wanneer een merkbeheerder gebruikmaakt van inloggen via een proxy. Dit maakt de impact van dit risico groot, omdat de imitator persoonsgegevens kan inzien en/of er toegang toe kan krijgen, wat mogelijk kan leiden tot ongeoorloofde toegang tot gegevens. Aangezien de

<sup>12</sup> Antwoorden van Qualtrics op vragen van SURF van 9 december 2025.

<sup>13</sup> Antwoorden van Qualtrics op SURF-vragen van 9 december 2025.

gebruiker noch voor noch na de sessie wordt geïnformeerd, moeten er meer maatregelen worden genomen om te voldoen aan het transparantiebeginsel uit artikel 5, lid 1, onder a), van de AVG. Dit maakt deze functie tot een groot risico voor betrokkenen.

De waarschijnlijkheid van dit risico is waarschijnlijker dan niet, aangezien de functie beschikbaar is zonder dat er meldingscontroles voor de eindgebruikers zijn. De functie wordt veelvuldig gebruikt, aangezien het een standaard ondersteuningsinstrument is.

### **C.2.8 Verlies van controle – interne systeem- en prestatielogboeken (Hoog)**

Tijdens het SURF-onderzoek is vastgesteld dat Qualtrics een logboek bijhoudt van interne systeem- en prestatiegebeurtenissen. Uit de documentatie van Qualtrics blijkt dat deze worden gebruikt voor het vastleggen van technische statistieken met betrekking tot de gezondheid van de infrastructuur, de integriteit van de dienstverlening en operationele afwijkingen. Bovendien bevatten de logboeken metagegevens zoals het IP-adres van de aanvrager, het gebruikte protocol en andere informatie die wordt vermeld in de sectie **'Error! Reference source not found.'** SURF heeft vastgesteld dat deze interne logboeken niet aan de klanten ter beschikking worden gesteld. Slechts een beperkte subset van activiteitsgegevens wordt aan klanten getoond via de gebruikersinterface van het platform of via API-eindpunten.

Wat de gevolgen betreft, zullen onderwijsinstellingen de verwerking van persoonsgegevens niet kunnen volgen en daardoor het overzicht verliezen over welke exacte persoonsgegevens door Qualtrics worden verwerkt, hetzij in de rol van verwerkingsverantwoordelijke, hetzij in die van verwerker. Als gevolg hiervan zullen onderwijsinstellingen, hoewel de verwerkingsverantwoordelijke overeenkomstig artikel 24 passende technische en organisatorische maatregelen moet treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG plaatsvindt, geen volledige controle hebben over de vraag of de metadata is opgenomen in de gegevensverwerking op het niveau van prestatielogboeken en zullen zij hun betrokkenen niet over deze verwerking kunnen informeren.

De kans dat de schade zich voordoet is waarschijnlijker dan niet, omdat Qualtrics op dit moment geen toegang verleent tot de persoonsgegevens in deze logbestanden.

Daarom wordt het risico als hoog ingeschat.

### **C.2.9 Verlies van controle: heridentificatie van gepseudonimiseerde gegevens – anonimiseringstechnieken voor het trainen van AI-modellen (Hoog)**

SURF constateerde een gebrek aan transparantie met betrekking tot het gebruik van 'eigen regels' en de afhankelijkheid van machine learning-technieken voor anonimisering. Het gebrek aan volledige controleerbaarheid bij Qualtrics en de mogelijkheid van geavanceerde heridentificatieaanvallen leiden tot een te grote afhankelijkheid van de interne processen van Qualtrics. Als er meer informatie over de interne processen beschikbaar zou zijn, zou het risico worden geminimaliseerd, omdat Qualtrics dan aan onderwijsinstellingen zou kunnen aantonen dat de leverancier voldoet aan de AVG en geen hoge gegevensverwerkingsrisico's met zich meebrengt.

De impact op betrokkenen is ernstig, omdat gevoelige persoonsgegevens (zoals specifiek Nederlandse identificatiegegevens) door het gebruik van geavanceerde inferentietechnieken blootgesteld zouden kunnen worden als re-identificatie plaatsvindt.

[REDACTED]

[REDACTED]

Bovendien beschikt Qualtrics niet over nauwkeurighedsstatistieken voor de anonimisering van Nederlandse gegevens, en kon het SURF evenmin meedelen of het model überhaupt op het Nederlands is getraind. Daarom blijft onduidelijk hoe de anonimiseringstechniek met het Nederlands werkt. Wat betreft de 'human in the loop' werden geen concrete statistieken gedeeld.

Daarnaast is een gerelateerd aspect aan het risico op heridentificatie dat SURF in de documentatie van Qualtrics niet kon verifiëren welke soorten AI-modellen Qualtrics gebruikt; er zijn geen gepubliceerde statistieken over de AI van Qualtrics. Daarom is het moeilijk om de effectieve anonimiseringstechnieken voor het trainen van AI-modellen te verifiëren. Hoewel leveranciers, naar de ervaring van SURF, deze informatie wel verstrekken om de effectiviteit van de anonimiseringstechnieken te bepalen.

De kans dat dit risico zich voordoet, neemt toe wanneer niet duidelijk wordt gecontroleerd of de anonimiseringstechnieken aan de vereisten voldoen. Een gebrek aan transparantie beperkt het vermogen van SURF en onderwijsinstellingen (verwerkingsverantwoordelijken) om risico's en compenserende maatregelen te beoordelen, wat aanzienlijke gevolgen heeft voor de betrokkenen. Hierdoor wordt de kans als hoog aangemerkt. SURF kan in haar conclusies niet overmatig vertrouwen op de interne processen van Qualtrics.

De kans dat schade ontstaat is waarschijnlijker dan niet, omdat betrokkenen zich niet bewust zijn van bepaalde gegevensverwerkingsactiviteiten. In de sectie '**Error! Reference source not found.**' heeft SURF de bevindingen van het technisch onderzoek gedeeld. De prestatie maatstaven komen niet overeen met hetzelfde detailniveau als leveranciers tijdens de DPIA's verstrekken.

Aangezien SURF beperkt inzicht heeft in de interne processen van Qualtrics en de waarschijnlijkheid van het risico hoog is zolang er onvoldoende transparantie is, wordt dit risico als hoog aangemerkt.

#### **C.2.10 Verlies van controle – Onvoldoende ondersteuning voor transparante communicatie met gebruikers en geïnformeerde toestemming (Hoog)**

Het risico hier is dat Qualtrics slechts een minimale standaard disclaimer biedt, waardoor de volledige verantwoordelijkheid bij onderwijsinstellingen (als verwerkingsverantwoordelijken) ligt om: gebruikers naar behoren te informeren over het verzamelen, gebruiken en bewaren van

gegevens en over hun rechten; geldige, geïnformeerde toestemming te verkrijgen; en te voldoen aan transparantieverplichtingen.

Zo ontbreekt in de cookie-toestemmingsbanner van Qualtrics een 'Alles weigeren'-optie, waardoor gebruikers in feite worden gestimuleerd om de gegevens te accepteren en het opt-outproces wordt bemoeilijkt. Nog kritischer is dat het platform cookies onmiddellijk bij het laden van de hoofdpagina inzet, nog voordat een gebruiker een keuze heeft gemaakt. Daardoor kunnen betrokkenen de verwerking van hun gedragsgegevens niet voorkomen, wat leidt tot een schending van de e-privacyrichtlijn en de transparantievereisten van de AVG.

De impact is groot, omdat er mogelijk ongeldige toestemming wordt verkregen als de mededelingen onduidelijk zijn over de bewaartermijnen van gegevens en de rechtsgrondslag voor de gegevensverwerking. De kans op schade is waarschijnlijker dan niet, omdat instellingen als verwerkingsverantwoordelijken vertrouwen op Qualtrics als gegevensverwerker en diens standaardinstellingen. Over het geheel genomen is het risico op ontoereikende ondersteuning voor transparante communicatie met gebruikers en geïnformeerde toestemming groot.

#### **C.2.11 Verlies van controle – Toestemmingsbanner en locatiegegevens (Hoog)**

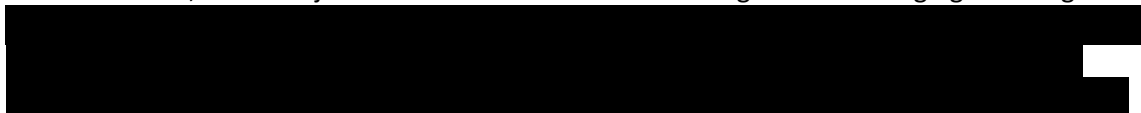
Een cruciaal aspect is de toewijzing van verantwoordelijkheid met betrekking tot de plaatsing van de toestemmingsbanner en het informeren van betrokkenen over het verzamelen van locatiegegevens. Qualtrics neemt een duidelijk standpunt in dat zij, als gegevensverwerker, geen directe interactie hebben met betrokkenen over deze technische gegevensverzameling. Bijgevolg rust de wettelijke verplichting om kennisgeving te doen en geldige toestemming te verkrijgen volledig bij de instelling (de verwerkingsverantwoordelijke).

De beschrijving van dit formaat luidt dat het gaat om een verborgen vraag waarmee informatie over de browser en het besturingssysteem wordt vastgelegd. Tijdens het technisch onderzoek constateerde SURF dat er locatiegegevens werden verzameld, wat niet op een duidelijke en concrete manier aan de gebruikers wordt uitgelegd. Deze aanpak is niet in overeenstemming met het beginsel van gegevensminimalisatie. Het verzamelen van IP-adressen en locatiegegevens is standaard ingeschakeld en beheerders moeten dit zelf uitschakelen. Bovendien wordt de toestemmingsbanner door de onderzoekers verstrekt, waardoor mogelijk niet alle verwerkingsactiviteiten daarin zijn opgenomen.

De impact op de betrokkenen is groot, omdat zij zich er tijdens het invullen van de enquête niet van bewust zijn welke gegevens worden verwerkt, en waarom het IP-adres van de eindgebruikers wordt verzameld en voor welke doeleinden. De kans op schade is waarschijnlijker dan niet, omdat dit een ingebouwde functie is die ertoe leidt dat er meer persoonsgegevens worden verzameld dan wettelijk is bekendgemaakt en die niet in overeenstemming is met de 'Privacy by Design'-keuzes. Over het geheel genomen wordt dit risico als hoog ingeschat.

#### **C.2.12 Onvoldoende bewijs van verzoeken tot verwijdering van het merk (opgelost)**

SURF heeft bevestigd dat Qualtrics beschikt over certificeringen van derde partijen, zoals ISO 27001 en SOC2, die redelijke zekerheid bieden met betrekking tot de beveiligingsmaatregelen.



[REDACTED]

[REDACTED]

De impact van dit risico werd voor betrokkenen als hoog beoordeeld. Indien tijdens het verwijderingsproces gegevens zijn verwijderd die volgens de wet nog moesten worden bewaard (gegevens met actieve licenties), bestaat het risico op verlies van persoonsgegevens die niet hadden mogen worden verwijderd, wat mogelijk gevolgen heeft voor betrokkenen die op deze gegevens vertrouwen.

[REDACTED] Het is belangrijk op te merken dat het herstel van de controle geen antwoord geeft op de openstaande vragen met betrekking tot de periode waarin de controle tekortschoot. Met name: wat er precies is gebeurd, welke betrokkenen of systemen hierdoor zijn getroffen en hoe lang de tekortkoming heeft geduurd. Deze vragen blijven relevant vanuit het perspectief van de verantwoordingsplicht en het incidentbeheer in het kader van de AVG en moeten afzonderlijk worden behandeld.

Wat betreft de huidige risicopositie: het nieuwe SOC 2-rapport van Qualtrics levert een positief resultaat op, en de door Qualtrics verstrekte herstelbrief beschrijft concrete tegenmaatregelen die zijn ontworpen om herhaling van het probleem te voorkomen. De onopgeloste vragen over de periode waarin de controle faalde, betekenen dat de verantwoordingsplicht voor die periode niet kan worden aangetoond.

[REDACTED] it risico vloeit voort uit de keuze van de leverancier voor het niveau van transparantie en nauwkeurigheid met betrekking tot zijn gegevensverwerkingsactiviteiten.

#### **C.2.13 Verlies van controle – Onvolledige geautomatiseerde detectie door ExpertReview van specifieke gevoelige identificatiegegevens van Nederlandse klanten in het onderwijs (Hoog)**

Het belangrijkste doel van het beleid inzake gevoelige gegevens is het beschermen van de privacy van respondenten door het identificeren en voorkomen van het verzamelen van gevoelige gegevens. Persoonsgegevens worden automatisch geblokkeerd en gemaskeerd via de

---

<sup>14</sup> Antwoorden van Qualtrics op de SURF-vragen van 9 december 2025.

<sup>15</sup> SOC 2 Type 2-rapport van Qualtrics over de systeem- en organisatiecontroles van Qualtrics met betrekking tot beveiliging, beschikbaarheid en vertrouwelijkheid (februari 2026).

functionaliteit van ExpertReview. Qualtrics fungeert als gegevensverwerker, en de merkbeheerder van de onderwijsinstelling definieert specifieke beleidsregels voor gevoelige gegevens door onderwerpen en vereisten in te stellen. Het huidige systeem detecteert echter niet automatisch voor Nederland specifieke gevoelige identificatiegegevens. Denk bijvoorbeeld aan Nederlandse mobiele telefoonnummers en het Nederlandse BSN (burgerservicenummer). Deze identificatiegegevens kunnen daarom worden verzameld zonder dat er waarschuwingen of maskeringen worden geactiveerd.

Merkbeheerders kunnen handmatig aangepaste detectieregels opstellen, maar het feit dat deze functie niet specifiek is afgestemd op Nederlandse onderwijsinstellingen heeft grote gevolgen voor de privacy. Het Nederlandse BSN wordt namelijk beschouwd als gevoelige persoonsgegevens volgens de AVG. Als deze gegevens niet worden gemaskeerd, kan het niet detecteren van deze identificatiegegevens leiden tot onrechtmatige verwerking en een inbreuk op de beginselen van gegevensminimalisatie.

De waarschijnlijkheid hangt af van de vraag of onderwijsinstellingen actief persoonsgegevens configureren via ExpertReview. Deze functie bevat een disclaimer waarin staat dat er geen garantie wordt gegeven voor gebruikers van talen die specifieke gegevens bevatten. De tool zal geen specifiek Nederlandse configuraties, zoals het BSN, kunnen detecteren. Hoewel onderwijsinstellingen hun eigen regels coderen en ervoor zorgen dat de tool in overeenstemming met de vastgestelde regels functioneert, is de kans dat het risico zich voordoet wanneer instellingen deze functie gebruiken groter dan dat het niet gebeurt. Want zelfs als deze functie niet actief door de instellingen wordt gebruikt, bestaat er een aanzienlijke kans dat bepaalde groepen betrokkenen die de functie gebruiken, hierdoor aanzienlijk worden beïnvloed.

Daarom wordt het risico als hoog ingeschat.

#### **C.2.14 Gebrek aan transparantie – geen publicatie van nauwkeurigheidsstatistieken voor het beleid inzake gevoelige gegevens en het ontbreken van feedbackmechanismen (Hoog)**

Het ontbreken van gepubliceerde nauwkeurigheidsstatistieken voor de detectie in het beleid inzake gevoelige gegevens ondermijnt het vermogen van onderwijsinstellingen om risico's met betrekking tot de betrouwbaarheid van het systeem te beoordelen en te beheren. Als gevolg hiervan zijn onderwijsinstellingen niet in staat om te beoordelen of gevoelige gegevens niet zijn gedetecteerd en daardoor zijn blootgesteld, of dat gevoelige gegevens ten onrechte zijn gemarkeerd of geredigeerd. Deze situatie wordt nog uitdagender door het ontbreken van feedback- en klachtenprocedures om onnauwkeurigheden in de detectie te melden.

De impact van dit risico is ernstig, omdat onderwijsinstellingen hierdoor moeite kunnen hebben om de nauwkeurigheid van gegevens en effectieve gegevensminimalisatie aan te tonen zonder bewijs van een nauwkeurig of onnauwkeurig detectiemechanisme.

Gezien de potentieel hoge waarschijnlijkheid en de complexiteit van het detecteren van gevoelige gegevens zonder gepubliceerde meetcriteria, moeten onderwijsinstellingen uitgaan van een matige kans op detectiefouten. Het ontbreken van feedback betekent dat fouten mogelijk gedurende langere tijd onopgemerkt blijven.

De combinatie van een grote impact en een hoge waarschijnlijkheid, gezien de gevoeligheid van persoonsgegevens, maakt dit tot een groot risico voor de gegevensbescherming.

#### **C.2.15 Verlies van controle en gebrek aan transparantie – Onvoldoende controle op vertaalde gebruikersenquêtes via Google Translate en Amazon Translate (Hoog)**

Het platform Qualtrics XM stuurt automatisch inhoud naar externe aanbieders van vertaaldiensten (Google Translate of Amazon Translate), zonder dat merkbeheerders de mogelijkheid hebben om dit gedrag uit te schakelen. Aanvankelijk informeerde Qualtrics gebruikers niet wanneer inhoud in de module Gegevensanalyse op deze manier werd verwerkt, noch waren er disclaimers over mogelijke onnauwkeurigheden in de vertaling.

Het risico dat gepaard gaat met het gebruik van vertaaldiensten van derden vergroot het risico op blootstelling van gegevens, omdat de tekst wordt verzonden naar externe serverproviders. Er zijn extra risico's wanneer gegevens zouden kunnen worden onderschept. Merkbeheerders hebben geen controle om deze gegevensuitwisseling uit te schakelen. Als gevolg hiervan kunnen onderwijsinstellingen niet voorkomen dat potentieel gevoelige gegevens standaard worden verzonden. Bovendien moeten eindgebruikers, volgens de sectie '**Error! Reference source not found.**', de automatische vertaling door andere vertaaldiensten handmatig inschakelen.

Qualtrics biedt de mogelijkheid om vertaalkolommen handmatig te hernoemen; hiervoor moet de gebruiker momenteel echter handmatig identificatiecodes ('AI-vertaald naar EN') aan het veld toevoegen. Deze maatregel maakt de kans dat het risico zich voordoet klein, mits onderwijsinstellingen de identificatiecodes aanpassen.

De kans dat er gebruik wordt gemaakt van automatische vertaaldiensten hangt af van de frequentie waarmee deze functie wordt gebruikt, namelijk of een onderzoeker op de vertaalknop klikt. De kans neemt toe naarmate er vaker enquêtes met gevoelige inhoud worden vertaald. Frequent gebruik van Google Translate en Amazon Translate betekent dat er herhaaldelijk gegevens worden blootgesteld, maar in beperkte mate. De kans dat er schade ontstaat is redelijk, omdat dit afhangt van hoe vaak betrokkenen de vertaling gebruiken.

De impact op de betrokkenen is ernstig, omdat er sprake is van verlies van controle over de nauwkeurigheid van de verwerking van persoonsgegevens.

#### **C.2.16 Doorgifte buiten de EU/EER – Automatisch gebruik van Google Translate en Amazon Translate (Hoog)**

Dit risico betreft het verlies van zeggenschap over de in de vorige paragraaf genoemde processen.

De impact op de betrokkenen is groot, omdat hun persoonsgegevens worden doorgegeven aan in de VS gevestigde hyperscalers (Google of Amazon) zonder de uitdrukkelijke toestemming van de betrokkene of tussenkomst van de verwerkingsverantwoordelijke (de onderwijsinstelling).

De kans op schade wordt als gemiddeld beschouwd, omdat deze alleen ontstaat wanneer een onderzoeker actief de 'Translate'-functie in de module Gegevensanalyse activeert. Aangezien de merkbeheerder deze functie echter niet globaal kan uitschakelen, kan de instelling niet

voorkomen dat een individuele onderzoeker per ongeluk of opzettelijk een niet-conforme doorgifte in gang zet.

Over het geheel genomen wordt dit risico als hoog ingeschat.

#### **C.2.17 Gebrek aan transparantie en ontbrekende toestemming als gevolg van onvolledige cookie-informatie (Hoog)**

In het hoofdstuk '**Error! Reference source not found.**' heeft SURF uitgelegd dat tijdens het technische onderzoek cookies zijn geïdentificeerd die niet in het cookiebeleid waren beschreven. De beschrijving van sommige geïdentificeerde cookies was niet opgenomen in de door Qualtrics genoemde artikelen. Dit gebrek aan transparantie beperkt het vermogen van onderwijsinstellingen als verwerkingsverantwoordelijken om de gebruikte cookies te beoordelen en al dan niet uitdrukkelijke toestemming te verlenen.

SURF heeft de 25 ontbrekende cookies die tijdens het technische onderzoek werden aangetroffen, nagegaan. Qualtrics heeft de doeleinden van de cookies toegelicht, maar deze doeleinden waren niet opgenomen in de cookieverklaring. Bovendien ontbraken ook de categorieën persoonsgegevens en de relevante subverwerkers in deze lijst.

De impact is ernstig omdat onderwijsinstellingen, zonder kennis van het doel van de verzamelde cookies en de relevante persoonsgegevens, mogelijk niet kunnen aantonen dat de rechtmatigheid van de gegevensverwerking wordt nageleefd. Krachtens de e-privacyrichtlijn is voor cookies de voorafgaande toestemming van de gebruiker vereist. Aangezien er geen informatie over de cookies wordt verstrekt, wordt er geen geldige toestemming verkregen. De kans op schade is waarschijnlijker dan niet, omdat het zich voordoet en dit leidt tot mogelijk onrechtmatige verwerking.

De ernstige impact en de matige waarschijnlijkheid maken dit risico groot voor betrokkenen en leiden tot onbedoelde inbreuken op de naleving door onderwijsinstellingen.

## Part D Beschrijving van voorgestelde risicobeperkende maatregelen

### D.1 Beperkende maatregelen

Het volgende gedeelte bevat een tabel met de technische, organisatorische en juridische risicobeperkende maatregelen die door de onderwijsinstelling of door Qualtrics moeten worden genomen om de geïdentificeerde 14 hoge risico's en 1 laag risico voor de betrokkenen te beperken.

Voor elk risico beschrijft de bovenste helft van de tabel het huidige risico en toont de risicoscore uit paragraaf C weer. In de onderste helft van de tabel worden de maatregelen beschreven die Xedule en de instellingen kunnen nemen en wordt een score voor het restrisico gegeven.

In het 'Afwijkend standpunt van Qualtrics' heeft SURF de 'Voorgestelde actie door Qualtrics' gedeeld, waarin de leverancier de ruimte kreeg om zijn visie te geven op de risicobeperkende maatregelen voor geïdentificeerde risico's, voor zover deze efficiënt en haalbaar worden geacht.

#### D.1.1 Verlies van controle – Contractuele rolbepaling

| Verlies van controle – Contractuele rolbepaling |                                                                                                                                                     |                                                                              |                           |               |                    |               |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------|---------------|--------------------|---------------|
| Referentie                                      | Oorzaak                                                                                                                                             | Gevolgen                                                                     | Waarschijnlijkheid        | Impact        | Risicoscore        | Huidig risico |
| Risico 1                                        | Afwijking tussen de juridische documentatie en de rol van de wederverkoper.                                                                         | Onderwijsinstellingen kunnen geschillen doorverwijzen naar de wederverkoper. | Laag                      | Laag          | Laag               | Huidig risico |
|                                                 | <b>Maatregelen instelling</b>                                                                                                                       | <b>Maatregelen leverancier</b>                                               | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> | Restrisico    |
|                                                 | Vermeld expliciet in de verwerkersovereenkomst dat meldingen van datalekken door de onderwijsinstellingen aan de leverancier moeten worden gericht. |                                                                              |                           |               | Laag               |               |
|                                                 | SURF stelt voor om een rechtstreekse verwerkersovereenkomst met Qualtrics te ondertekenen.                                                          |                                                                              |                           |               |                    |               |

|  |                                                                                                                                                                                                                                                                                           |  |  |  |  |  |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | Indien een rechtstreekse verwerkersovereenkomst niet haalbaar of mogelijk is, voeg dan een addendum toe aan de huidige overeenkomst waarin wordt vastgelegd dat Qualtrics de enige verwerker is. [REDACTED] dient te worden aangemerkt als een 'reseller' of 'commerciële tussenpersoon'. |  |  |  |  |  |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|

#### D.1.2 Verlies van controle – een gegevensagnostische aanpak die de rolverdeling tussen de partijen en het beginsel van doelbinding ondermijnt

| Verlies van controle – gegevensagnostische benadering |                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                 |                    |          |             |               |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------|-------------|---------------|
| Referentie                                            | Oorzaak                                                                                                                                                                                                                                                                                                                                | Gevolgen                                                                                                                                                                        | Waarschijnlijkheid | Gevolgen | Risicoscore |               |
| Risico 2                                              | Door de gegevensneutrale aanpak hoeft Qualtrics geen specifieke details over de gegevensverwerking te verstrekken.                                                                                                                                                                                                                     | De leverancier belemmert onderwijsinstellingen om de naleving van doelbinding en gegevensminimalisatie te controleren.                                                          | Hoog               | Hoog     | Hoog        | Huidig risico |
|                                                       | Maatregelen instelling                                                                                                                                                                                                                                                                                                                 | Maatregelen leverancier                                                                                                                                                         | Waarschijnlijkheid | Gevolgen | Risicoscore | Restrisico    |
|                                                       | Aangezien de leverancier geen categorieën verstrekt, moet de instelling strikte 'gegevensrecords' invoeren voor eindgebruikers zoals onderzoekers, medewerkers of studenten. Door te beperken welke velden op het platform kunnen worden aangemaakt, kan de instelling de categorieën van gegevens en betrokkenen 'zelf documenteren'. | Modulaire openbare pagina met specifieke informatie over de gebruikelijke categorieën gegevens die worden verwerkt en de doeleinden waaraan de persoonsgegevens zijn gekoppeld. |                    |          | Laag        |               |
|                                                       |                                                                                                                                                                                                                                                                                                                                        | Maak een duidelijk onderscheid tussen welke gegevens door Qualtrics worden verwerkt als verwerkingsverantwoordelijke en/of gegevensverwerker.                                   |                    |          |             |               |
|                                                       | Zorg ervoor dat alleen de 'geïnformeerde' kernverwerking plaatsvindt.                                                                                                                                                                                                                                                                  | Onderhandel met onderwijsinstellingen en neem in de verwerkersovereenkomst een expliciete bepaling op die 'geen AI/LLM-training op basis van de verwerking van                  |                    |          |             |               |
|                                                       |                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                 |                    |          |             |               |

|  |                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                |  |  |  |  |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|
|  | Het gebruik van het platform voor bijzondere categorieën gegevens verbieden.                                                                                                                                                         | de gegevens van de klant' toestaat.                                                                                                                                                                                                                                            |  |  |  |  |
|  | Onderwijsinstellingen moeten een expliciete 'verbodsbepaling inzake AI/LLM-training op basis van de verwerking van de gegevens van de klant' hebben.                                                                                 | Leg contractueel de absolute anonimisering (niet alleen pseudonimisering) vast voor alle gegevens die worden gebruikt voor 'Onderzoek en ontwikkeling' of 'Productverbetering'. Geef onderwijsinstellingen de mogelijkheid om zich af te melden voor de anonimisatieprocessen. |  |  |  |  |
|  | Zorg ervoor dat in de eigen privacyverklaring van de onderwijsinstelling expliciet de categorieën persoonsgegevens worden vermeld die de leverancier verwerkt als gegevensverwerker en, eventueel, als verwerkingsverantwoordelijke. | Breng de categorieën persoonsgegevens die Qualtrics verwerkt in kaart in overeenstemming met de 7 doeleinden waarvoor Qualtrics als verwerkingsverantwoordelijke optreedt                                                                                                      |  |  |  |  |
|  | In Bijlage 1 moeten de categorieën persoonsgegevens aan de doeleinden worden gekoppeld.                                                                                                                                              | Publiceer een openbare gegevenstoewijzing voor alle Qualtrics-producten waarin elke mogelijke categorie verzamelde persoonsgegevens wordt vermeld.                                                                                                                             |  |  |  |  |
|  |                                                                                                                                                                                                                                      | Zorg voor een transparantiedashboard waarmee de beheerder kan zien welke categorieën precies worden gebruikt, bijvoorbeeld voor de ontwikkeling van diensten.                                                                                                                  |  |  |  |  |
|  |                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                |  |  |  |  |

### D.1.3 Onvermogen om de rechten van betrokkenen uit te oefenen – Transparantiekwestie met betrekking tot de DSAR-ondersteuning voor instellingen

| Onvermogen om de rechten van betrokkenen uit te oefenen – Transparantiekwestie met betrekking tot de ondersteuning van instellingen bij verzoeken om inzage |                                                                                                                                                                                                                                                                              |                                                                                                                       |                           |               |                    |                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|----------------------|
| Referentie                                                                                                                                                  | Oorzaak                                                                                                                                                                                                                                                                      | Gevolgen                                                                                                              | Waarschijnlijkheid        | Impact        | Risicoscore        |                      |
| <b>Risico 3</b>                                                                                                                                             | Hoewel de antwoorden op de enquête toegankelijk zijn, ontbreekt de loginformatie.                                                                                                                                                                                            | Nu de DSAR-tool wordt verbeterd, kan de aanvullende loginformatie dit risico mogelijk beperken.                       | <b>Gemiddeld</b>          | <b>Hoog</b>   | <b>Hoog</b>        | <b>Huidig risico</b> |
|                                                                                                                                                             | <b>Maatregelen instelling</b>                                                                                                                                                                                                                                                | <b>Maatregelen leverancier</b>                                                                                        | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> | <b>Restrisico</b>    |
|                                                                                                                                                             | Wanneer in het DSAR-antwoord bepaalde categorieën gegevens ontbreken, moet er binnen de instelling een formele procedure worden ingesteld waarbij een handmatig ticket naar de Qualtrics-helpdesk wordt gestuurd waarin specifiek om de ontbrekende gegevens wordt gevraagd. | Qualtrics moet de ontbrekende loggegevens toevoegen en het volledige DSAR-antwoord naar onderwijsinstellingen sturen. |                           |               | <b>Laag</b>        |                      |
|                                                                                                                                                             | Stel een handleiding op voor eindgebruikers (beheerders, studenten en anderen) over een bijgewerkte DSAR-tool.                                                                                                                                                               |                                                                                                                       |                           |               |                    |                      |

### D.1.4 Gebrek aan transparantie in de lijst met subverwerkers – Onvolledige lijst met subverwerkers

| Gebrek aan transparantie in de lijst met subverwerkers – Onvolledige lijst met subverwerkers |                                                                          |                                                                                                                |                           |               |                    |                      |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|----------------------|
| Referentie                                                                                   | Oorzaak                                                                  | Gevolgen                                                                                                       | Waarschijnlijkheid        | Impact        | Risicoscore        |                      |
| <b>Risico 4</b>                                                                              | De kern van dit risico is de niet-bekendgemaakte verwerking door derden. | Onderwijsinstellingen geven gegevens onbewust door aan entiteiten die niet als subverwerkers zijn goedgekeurd. | <b>Hoog</b>               | <b>Hoog</b>   | <b>Hoog</b>        | <b>Huidig risico</b> |
|                                                                                              | <b>Maatregelen instelling</b>                                            | <b>Maatregelen leverancier</b>                                                                                 | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> | <b>Restrisico</b>    |
|                                                                                              | Vraag de leverancier om de volledige lijst met subverwerkers en doe dit  | Voeg de genoemde subverwerkers toe aan de lijst met subverwerkers.                                             |                           |               | <b>Laag</b>        |                      |

|  |                                                                                                                                                                                                                  |                                                                                                                   |  |  |  |  |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--|--|--|--|
|  | <p>periodiek binnen een onderwijsinstelling.</p> <p>Schakel de functies uit die verband houden met de verwerking door derden, totdat de leverancier een duidelijke beschrijving van het doel ervan toevoegt.</p> | Bied een opt-out aan waarmee instellingen alle telemetrie door derden voor de eindgebruikers kunnen uitschakelen. |  |  |  |  |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--|--|--|--|

#### D.1.5 Gebrek aan transparantierapporten

| Gebrek aan transparantierapporten |                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                               |                    |        |             |               |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                        | Oorzaak                                                                                                                                                                                                                                                                                                                                                   | Gevolgen                                                                                                                                                                                                                                                                                                      | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risico 6                          | Het risico vloeit voort uit de informatieasymmetrie tussen de aanbieder en het publiek.                                                                                                                                                                                                                                                                   | Zonder openbare gegevens over verzoeken van overheden kunnen instellingen niet nagaan of zij het voorwerp zijn van onevenredige surveillance, met name door autoriteiten buiten de EU.                                                                                                                        | Hoog               | Hoog   | Hoog        | Huidig risico |
|                                   | Maatregelen instelling                                                                                                                                                                                                                                                                                                                                    | Maatregelen leverancier                                                                                                                                                                                                                                                                                       | Waarschijnlijkheid | Impact | Risicoscore | Restrisico    |
|                                   | Hoewel het specifieke Qualtrics-rapport vertrouwelijk kan zijn, kan de instelling een algemene verklaring opnemen in haar eigen openbare transparantierapport. Bijvoorbeeld: <i>'Onze leveranciers hebben gemeld dat er in het afgelopen kalenderjaar geen verzoeken om gegevensopenbaarmaking zijn ontvangen van buitenlandse inlichtingendiensten.'</i> | <p>Lanceer een webpagina met geaggregeerde, geanonimiseerde statistieken over verzoeken van overheden wereldwijd. Deze moeten het volgende bevatten:</p> <p>Aantal ontvangen verzoeken;</p> <p>Het percentage verzoeken dat is aangevochten of afgewezen;</p> <p>Categorieën van de opgevraagde gegevens.</p> |                    |        | Laag        |               |

#### D.1.6 Gebrek aan transparantie – Inloggen via een proxy

| Verlies van controle – interne systeem- en prestatie-logboeken |                                            |                                                                                           |                    |        |             |               |
|----------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                     | Oorzaak                                    | Gevolgen                                                                                  | Waarschijnlijkheid | Impact | Risicoscore | Huidig risico |
| Risico 7                                                       | Via proxy-aanmelding kunnen merkbeheerders | Het ongeoorloofd inzien van persoonsgegevens kan regelmatig en herhaaldelijk plaatsvinden | Hoog               | Hoog   | Hoog        |               |

|  |                                                                                                      |                                                                                                                                                                            |                           |               |                    |  |
|--|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|--|
|  | toegang krijgen tot accounts van eindgebruikers zonder dat deze hiervan op de hoogte worden gesteld. | zonder dat de betrokkene hiervan op de hoogte is.                                                                                                                          |                           |               |                    |  |
|  | <b>Maatregelen Instelling</b>                                                                        | <b>Maatregelen Leverancier</b>                                                                                                                                             | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> |  |
|  | Proxy-aanmelding uitschakelen                                                                        | Implementeer realtime meldingen voor eindgebruikers Dit moet bijvoorbeeld niet alleen zichtbaar zijn voor de beheerder, maar ook voor de gebruikers die worden gemaskeerd. |                           |               |                    |  |
|  |                                                                                                      | Op rollen gebaseerde beperkingen: beperk de toegang van een imitator tijdens een sessie.                                                                                   |                           |               | Laag               |  |

#### D.1.7 Verlies van controle – interne systeem- en prestatie-logboeken

| Verlies van controle – interne systeem- en prestatie-logboeken |                                                                                                                                                           |                                                                                                                                                                                                                           |                           |               |                    |               |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|---------------|
| Referentie                                                     | Oorzaak                                                                                                                                                   | Gevolgen                                                                                                                                                                                                                  | Waarschijnlijkheid        | Impact        | Risicoscore        |               |
|                                                                | Qualtrics registreert technische statistieken en metagegevens in logbestanden die voor de klant niet toegankelijk zijn.                                   | Omdat instellingen deze logbestanden niet kunnen inzien, controleren of exporteren, kunnen ze voor deze specifieke dataset niet 'aantonen dat ze voldoen' aan de beginselen van gegevensminimalisatie of opslagbeperking. | Hoog                      | Hoog          | Hoog               | Huidig risico |
|                                                                | <b>Maatregelen instelling</b>                                                                                                                             | <b>Maatregelen leverancier</b>                                                                                                                                                                                            | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> |               |
| <b>Risico 8</b>                                                | Vermeld expliciet in de verwerkersovereenkomst dat prestatie-logboeken deel uitmaken van de gegevenscategorie in Bijlage 1 van de verwerkersovereenkomst. | Publiceer een lijst voor klanten waarin precies wordt vermeld welke metagegevens in prestatie-logboeken worden vastgelegd.<br><br>Verstrek een volledige kopie van de persoonsgegevens (inclusief het volledige DSAR).    |                           |               | Laag               |               |

**D.1.8 Verlies van controle: heridentificatie van gepseudonimiseerde gegevens – anonimiseringstechnieken voor het trainen van AI-modellen**

| Gebrek aan transparantie – anonimiseringstechnieken voor het trainen van AI-modellen |                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                           |               |                    |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|
| Referentie                                                                           | Oorzaak                                                                                                                                                                                                   | Gevolgen                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Waarschijnlijkheid        | Impact        | Risicoscore        |
| <b>Risico 9</b>                                                                      | Het risico heeft betrekking op de 'black box'-benadering van de door de leverancier gebruikte anonimiseringstechnieken.                                                                                   | Geanonimiseerde gegevens worden gebruikt voor het trainen van modellen, maar bieden geen bewijs van de nauwkeurigheid of juridische geldigheid van deze technieken, met name voor de Nederlandse taal.                                                                                                                                                                                                                                                                               | Hoog                      | Hoog          | Hoog               |
|                                                                                      | <b>Maatregelen instelling</b>                                                                                                                                                                             | <b>Maatregelen leverancier</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> |
|                                                                                      | Voeg een strikte clause toe aan de verwerkersovereenkomst waarin wordt bepaald dat het anonimiseren en aggregeren van institutionele gegevens voor AI-training of productverbetering strikt verboden is.  | Qualtrics moet een lijst publiceren met de gegevenstypen die het ML-model is getraind om te detecteren.<br><br>Qualtrics moet transparanter zijn over de Nederlandse prestatiestatistieken. Wees transparanter over de Nederlandse prestatiestatistieken en leg de drempels en maatstaven uit voor de menselijke tussenkomst.<br><br>Leg uit en toon het percentage/de meetwaarden van door AI geanonimiseerde gegevens die handmatig worden gecontroleerd door menselijke auditors. |                           |               | Laag               |
|                                                                                      | Vraag formeel om een rapport over de meetwaarden voor de Nederlandse taal. Als de leverancier deze niet kan verstrekken, moet de instelling ervan uitgaan dat de anonimisering technisch ontoereikend is. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                           |               |                    |
|                                                                                      |                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                           |               | Restrisico         |

|  |                                                                                                                                                                                                                                                          |  |  |  |  |  |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | Gebruik de instellingen van de merkbeheerder om alle generatieve AI-functies en geautomatiseerde inzichten globaal uit te schakelen totdat de leverancier een transparantiewitboek verstrekt met een lijst van alle gegevensvelden die worden geschoond. |  |  |  |  |  |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|

#### D.1.9 Verlies van controle – Onvoldoende ondersteuning voor transparante communicatie met gebruikers en geïnformeerde toestemming

| Onvoldoende ondersteuning voor transparante communicatie met gebruikers en geïnformeerde toestemming |                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                              |                    |        |             |               |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                                                           | Oorzaak                                                                                                                                                                                            | Gevolgen                                                                                                                                                                                                                                                                                                                                                                                     | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risico 10                                                                                            | De standaard cookiebanner van Qualtrics heeft doorgaans geen 'Alles weigeren'-knop op de eerste laag.                                                                                              | Onderwijsinstellingen verkrijgen onbewust 'ongeldige toestemming' van betrokkenen, waardoor elke verdere gegevensverwerking onrechtmatig is vanaf het moment dat de pagina wordt geladen.                                                                                                                                                                                                    | Hoog               | Hoog   | Hoog        | Huidig risico |
|                                                                                                      | Maatregelen Instelling                                                                                                                                                                             | Maatregelen leverancier                                                                                                                                                                                                                                                                                                                                                                      | Waarschijnlijkheid | Impact | Risicoscore | Res risico    |
|                                                                                                      | Stel een specifiek toestemmingsformulier op.                                                                                                                                                       | Werk het algemene platformthema bij zodat er standaard een 'Alles afwijzen'-knop in zit, in plaats van dat er aangepaste code van de klant nodig is.                                                                                                                                                                                                                                         |                    |        | Laag        |               |
|                                                                                                      | Geef onderzoekers de instructie om deze toestemmingsformulieren toe te voegen en in te vullen als er meta-informatie wordt gebruikt (naast andere vragen die mogelijk persoonsgegevens onthullen). | Herontwerp het toegangspunt van het platform zodat er geen niet-essentiële cookies (analytics, functionele voorkeuren) worden geplaatst totdat de toestemmings-API een positief signaal van de gebruiker ontvangt.<br><b>(Qualtrics heeft aan SURF laten weten dat de leverancier zal onderzoeken hoe het toegangspunt kan worden aangepast. Er zijn geen concrete toezeggingen gedaan).</b> |                    |        |             |               |

#### D.1.10 Verlies van controle – Toestemmingsbanner en locatiegegevens

##### Verlies van controle – Meta-informatie

| Referentie | Oorzaak                                                                                                                                                                                                                                                                   | Gevolgen                                                                                                                                                                                         | Waarschijnlijkheid | Impact | Risicoscore |               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Risico 11  | Geen toestemmingsbanner en het verzamelen van locatiegegevens.                                                                                                                                                                                                            | Onderwijsinstellingen verkrijgen onbewust 'ongeldige toestemming' van betrokkenen, waardoor elke daaropvolgende gegevensverwerking onrechtmatig is vanaf het moment dat de pagina wordt geladen. | Hoog               | Hoog   | Hoog        | Huidig risico |
|            | Maatregelen instelling                                                                                                                                                                                                                                                    | Maatregelen leverancier                                                                                                                                                                          | Waarschijnlijkheid | Impact | Risicoscore | Restrisico    |
|            | Stel een specifiek toestemmingsformulier op.<br><br>Geef onderzoekers de opdracht om toestemmingsformulieren op te stellen en informeer de onderzoekers over de verwerking van locatiegegevens (naast andere vragen die mogelijk persoonsgegevens aan het licht brengen). | Ontwerp de maatregel zodanig dat niet-essentiële cookies (analytics, functionele voorkeuren) niet worden geplaatst totdat de toestemmings-API een positief signaal van de gebruiker ontvangt.    |                    |        | Laag        |               |

#### D.1.11 Onvoldoende bewijs van verzoeken tot verwijdering van het merk (opgelost)

| Onvoldoende bewijs van de verzoeken tot verwijdering van het merk |                                                                                                                                                             |                                                                                                   |                    |        |             |               |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                        | Oorzaak                                                                                                                                                     | Gevolgen                                                                                          | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risico 12                                                         |                                                                                                                                                             | Dit leidt tot een compliance-tekortkoming die Qualtrics begin 2026 heeft verholpen en aangetoond. | Op afstand         | Hoog   | Op afstand  | Huidig risico |
|                                                                   | Maatregelen instelling                                                                                                                                      | Maatregelen leverancier                                                                           | Waarschijnlijkheid | Impact | Risicoscore | Restrisico    |
|                                                                   | Qualtrics heeft aangegeven dat er begin 2026 een nieuw rapport beschikbaar zal zijn. Instellingen dienen dit document formeel op te vragen om te verifiëren | Het nieuwe SOC2-rapport is beschikbaar.                                                           |                    |        |             |               |

|  |                                                                           |  |  |  |  |
|--|---------------------------------------------------------------------------|--|--|--|--|
|  | <div></div> <p>zijn getest en bevestigd door onafhankelijke auditors.</p> |  |  |  |  |
|--|---------------------------------------------------------------------------|--|--|--|--|

#### D.1.12 Verlies van controle – Onvolledige geautomatiseerde detectie door ExpertReview van specifieke gevoelige identificatiegegevens voor Nederlandse klanten in het onderwijs

| Onvolledige geautomatiseerde detectie door ExpertReview van specifieke gevoelige identificatiegegevens voor Nederlandse klanten in het onderwijs |                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                               |                    |        |             |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|
| Referentie                                                                                                                                       | Oorzaak                                                                                                                                                                                                                                                                                   | Gevolgen                                                                                                                                                                                                      | Waarschijnlijkheid | Impact | Risicoscore |
| Risico 13                                                                                                                                        | De functie 'Beleid voor gevoelige gegevens' mist vooraf geconfigureerde 'onderwerpen' voor specifiek Nederlandse identificatiegegevens, waardoor deze functie zijn doel voor instellingen in Nederland niet vervult.                                                                      | Zeer gevoelige gegevens, zoals het BSN (Burgerservicenummer) of Nederlandse mobiele nummers, kunnen worden verzameld zonder dat het systeem een waarschuwing geeft.                                           | Hoog               | Hoog   | Hoog        |
|                                                                                                                                                  | Maatregelen instelling                                                                                                                                                                                                                                                                    | Maatregelen leverancier                                                                                                                                                                                       | Waarschijnlijkheid | Impact | Risicoscore |
|                                                                                                                                                  | Stel het 'Beleid inzake gevoelige gegevens' in om gevoelige informatie uit enquêtereacties te verbergen. Dit zorgt ervoor dat, zelfs als een respondent uit eigen beweging zijn BSN in een open tekstveld invoert, de gegevens worden vervangen door sterretjes of een andere vervanging. | Verbeter Text iQ en ExpertReview zodat ze Nederlandse aanduidingen voor gevoelige gegevens kunnen herkennen. Zo zal het herkennen van een BSN bijvoorbeeld leiden tot waarschuwingen voor gevoelige gegevens. |                    |        | Laag        |

|  |                                                                                                               |  |  |  |  |  |
|--|---------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | Configureer geen persoonsgegevens via ExpertReview, totdat Qualtrics de beschreven maatregel heeft uitgevoerd |  |  |  |  |  |
|--|---------------------------------------------------------------------------------------------------------------|--|--|--|--|--|

#### D.1.13 Gebrek aan transparantie – geen publicatie van nauwkeurigheidsstatistieken voor het beleid inzake gevoelige gegevens en het ontbreken van feedbackmechanismen

| Gebrek aan transparantie – geen publicatie van nauwkeurigheidsstatistieken voor het beleid inzake gevoelige gegevens en het ontbreken van feedbackmechanismen |                                                                                    |                                                                                                                                                                                                                                                                                                                      |                    |        |             |               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                                                                                                                    | Oorzaak                                                                            | Gevolgen                                                                                                                                                                                                                                                                                                             | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risiko 14                                                                                                                                                     | Het kernprobleem is het gebrek aan transparantie met betrekking tot de prestaties. | Er is geen feedbackknop in de interface voor het opstellen van enquêtes. Dit leidt tot een feedbacktekort voor de instellingen.                                                                                                                                                                                      | Hoog               | Hoog   | Hoog        | Huidig risico |
|                                                                                                                                                               | Maatregelen instelling                                                             | Maatregelen leverancier                                                                                                                                                                                                                                                                                              | Waarschijnlijkheid | Impact | Risicoscore | Resrisico     |
|                                                                                                                                                               | Dien tickets of supportverzoeken in bij Qualtrics voor de feedback.                | Qualtrics dient deel te nemen aan kwartaaloverleggen om bekende detectiehiaten te bespreken en samen met SURF een stappenplan op te stellen voor het verbeteren van de identificatie specifiek voor Nederland.<br><br>Voeg direct een knop 'markeren als onnauwkeurig' toe aan het beleid inzake gevoelige gegevens. |                    |        | Laag        |               |

#### D.1.14 Verlies van controle – Automatisch gebruik van Google Translate en Amazon Translate

| Verlies van controle – Automatisch gebruik van Google Translate en Amazon Translate |                                                                                                                                  |                                                                                                                      |                    |        |             |               |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                                          | Oorzaak                                                                                                                          | Gevolgen                                                                                                             | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risiko 15                                                                           | Ongecontroleerde gegevensstroom naar subverwerkers die niet rechtstreeks worden beheerd door de merkbeheerder van de instelling. | De verwerking van gegevens via de automatische vertaaldiensten van Google en Amazon duidt op een gegevensoverdracht. | Gemiddeld          | Hoog   | Hoog        | Huidig risico |

|  | Maatregelen instelling                                                                                                     | Maatregelen leverancier                                                                                               | Waarschijnlijkheid | Impact | Risicoscore |                    |
|--|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|--------------------|
|  | Een handmatige handeling die de gebruiker die vertaalt moet uitvoeren (bijv. 'AI vertaald naar EN' toevoegen) in het veld. | Qualtrics zal een ingebouwde functie bieden waarmee de instelling handmatig gebruik kan maken van de vertaaldiensten. |                    |        | Laag        | Res<br>trisi<br>co |

#### D.1.15 Overdracht buiten de EU/EER – Automatisch gebruik van Google Translate en Amazon Translate

| Gebrek aan transparantie en ontbrekende toestemming als gevolg van onvolledige cookie-informatie |                                                                                                                                           |                                                                                                                                                      |                    |        |             |                    |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------|-------------|--------------------|
| Referentie                                                                                       | Oorzaak                                                                                                                                   | Gevolgen                                                                                                                                             | Waarschijnlijkheid | Impact | Risicoscore |                    |
| Risico 16                                                                                        | Ongecontroleerde gegevensstroom naar subverwerkers in de VS die niet rechtstreeks worden beheerd door de merkbeheerder van de instelling. | De verwerking van gegevens via de automatische vertaaldiensten van Google en Amazon duidt op een gegevensoverdracht buiten de EU/EER.                | Gemiddeld          | Hoog   | Hoog        | Huidig risico      |
|                                                                                                  | Maatregelen instelling                                                                                                                    | Maatregelen leverancier                                                                                                                              | Waarschijnlijkheid | Impact | Risicoscore |                    |
|                                                                                                  | De eindgebruikers informeren over de vertaalfunctie.                                                                                      | Bied een andere vertaaloptie aan: Europese alternatieven.<br><br>Bied merkbeheerders de mogelijkheid om handmatig extra vertaalopties toe te voegen. |                    |        | Laag        | Res<br>trisi<br>co |

#### D.1.16 Gebrek aan transparantie en ontbrekende toestemming als gevolg van onvolledige cookie-informatie

| Gebrek aan transparantie en ontbrekende toestemming als gevolg van onvolledige cookie-informatie |                                                                                                                                                                                                                                |                                                                             |                    |        |             |               |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|--------------------|--------|-------------|---------------|
| Referentie                                                                                       | Oorzaak                                                                                                                                                                                                                        | Gevolgen                                                                    | Waarschijnlijkheid | Impact | Risicoscore |               |
| Risico 17                                                                                        | Zonder een volledige en nauwkeurige lijst van cookies is elke toestemming die van een student of onderzoeker is verkregen technisch gezien ongeldig, aangezien zij niet 'geïnformeerd' kunnen worden over tracking waarvan zij | De betrokkenen zullen zich niet bewust zijn van de verwerkingsactiviteiten. | Hoog               | Hoog   | Hoog        | Huidig risico |

|  |                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                           |               |                    |                             |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------|--------------------|-----------------------------|
|  | het bestaan niet kennen.                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                           |               |                    |                             |
|  | <b>Maatregelen instelling</b>                                                                                                                                                      | <b>Maatregelen leverancier</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Waarschijnlijkheid</b> | <b>Impact</b> | <b>Risicoscore</b> |                             |
|  | Geef de leverancier een formele instructie om alle cookies die zijn aangemerkt als 'Marketing' of 'Targeting' en die niet strikt noodzakelijk zijn voor de dienst, te deactiveren. | <p>Qualtrics moet een realtime, machinaal leesbare lijst verstrekken van alle cookies die momenteel in gebruik zijn. Hierdoor kunnen onderwijsinstellingen hun eigen transparantieverklaringen automatisch bijwerken telkens wanneer de leverancier een nieuwe tracker toevoegt.</p> <p>Voor elke gebruikte cookie moet Qualtrics een duidelijke technische motivering geven waaruit blijkt dat deze 'strikt noodzakelijk' is in de zin van artikel 5, lid 3, van de e-privacyrichtlijn.</p> |                           |               | Laag               | <b>Res<br/>trisi<br/>co</b> |

## Conclusie

Deze DPIA heeft 14 hoge en 1 laag risico geïdentificeerd in verband met het gebruik van Qualtrics Design XM for Education. Wat betreft de in deel D door SURF voorgestelde risicobeperkende maatregelen, kunnen onderwijsinstellingen de door SURF voorgestelde maatregelen bekijken om sommige van de risico's te beperken. Deze maatregelen hebben betrekking op lage risico's en functies die door de instellingen kunnen worden uitgeschakeld. Het is onwaarschijnlijk dat de hoge risico's kunnen worden opgelost zonder vaste en concrete toezeggingen van Qualtrics om passende technische en organisatorische maatregelen op leveranciersniveau te implementeren.

Gedurende het gehele DPIA-proces heeft SURF voortdurend gestreefd naar het best mogelijke resultaat van de DPIA en in elke fase van het project overleg gepleegd met Qualtrics. Hoewel Qualtrics in de beginfase van de beoordeling niet actief betrokken was, heeft de beoordeling door Qualtrics van de voltooide DPIA en de geïdentificeerde risico's geleid tot het besef dat een meer substantiële deelname van waarde is. De leverancier heeft zich niet verbonden tot het implementeren van risicobeperkende maatregelen en heeft de risicoclassificatie van SURF betwist.

De geïdentificeerde hoge risico's hebben betrekking op het volgende: de gegevensagnostische aanpak, een onvolledige lijst van subverwerkers, verlies van controle en transparantie als gevolg van het onvolledig verzamelen van toestemming, onvolledige cookielijsten en een onvolledige afhandeling van de DSAR's.

Het doel van SURF is ervoor te zorgen dat het gebruik van de producten van Qualtrics door onderwijsinstellingen in Nederland volledig in overeenstemming is met de AVG. SURF loopt voorop bij het uitvoeren en publiceren van de resultaten van DPIA's namens haar leden. Gezien de geïdentificeerde, nog niet opgeloste hoge risico's dringt SURF er bij onderwijsinstellingen op aan om de bevindingen van deze DPIA zorgvuldig in overweging te nemen alvorens het platform van Qualtrics te blijven gebruiken.

Mocht Qualtrics concrete toezeggingen doen om de nodige risicobeperkende maatregelen te nemen, dan zal SURF deze beoordeling dienovereenkomstig aanpassen.