SAMENVATTING

RAND EUROPE



Identiteits- en documentfraude in de context van kennisveiligheid

Internationale casestudies en lessen voor Nederland

Judith Huismans, Scott Warnier, Conlan Ellis, Fook Nederveen

Dit onderzoek werd gefinancierd door het Wetenschappelijk Onderzoek- en Datacentrum (WODC).

For more information on this publication, visit www.rand.org/t/RRA5003-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© 2026 RAND Corporation

RAND® is a registered trademark.

Cover image: Adobe Stock

Limited Print and Electronic Distribution Rights
This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorised posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

© 2026 RAND Europe. Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van RAND Europe.

Samenvatting

Internationale samenwerking en het aantrekken van talent zijn cruciaal voor de wetenschappelijke en economische vooruitgang van Nederland. Tegelijkertijd uit de overheid zorgen over toenemende veiligheidsdreigingen vanuit landen die gericht proberen waardevolle kennis en technologie uit Nederland te verkrijgen.[1] China wordt in recente dreigingsanalyses steevast genoemd als de voornaamste bedreiging vanwege het verweven beleid van kennis- en innovatieverwerving in dienst van de nationale veiligheid en defensie.[2] Dit uit zich onder meer in grootschalige spionageprogramma's en het financieren van studenten en onderzoekers om toegang te krijgen tot geavanceerde technologieën. Dergelijke activiteiten bedreigen niet alleen de kennisveiligheid van onderwijs- en onderzoeksinstellingen, maar ook de innovatiekracht van bedrijven, de effectiviteit van de krijgsmacht en de strategische autonomie van Nederland.[3]

Het tegengaan van ongewenste kennisoverdracht en strategische afhankelijkheden vraagt om een sterk kennisveiligheidsbeleid.

Doelstellingen en onderzoeksopzet

Tegen deze achtergrond is er behoefte aan verdiepend onderzoek naar het beleid en de praktijk rond kennisveiligheid, specifiek gericht op de risico's van identiteits- en documentfraude binnen de Nederlandse kennissector. Gedocumenteerde casuïstiek is schaars, wat het lastig maakt om effectief en proportioneel beleid te ontwikkelen. Lessen uit de praktijk over de inzet van identiteits- en documentatiefraude om toegang te krijgen tot sensitieve technologie en kennis kunnen niettemin belangrijke inzichten opleveren voor het ontwikkelen van een uitvoerbaar en efficiënt screeningsproces. Op aanvraag van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft het Wetenschappelijk Onderzoek- en Datacentrum (WODC) daarom aan RAND Europe gevraagd om te analyseren hoe screening op identiteits- en documentfraude in Nederland en een selectie van andere landen is georganiseerd, welke vormen van fraude voorkomen, hoe frequent deze zich voordoen en welke waarborgen effectief zijn om deze risico's tegen te gaan.

Het onderzoek omvat een literatuurstudie naar de wijze waarop en de frequentie waarmee identiteits- en documentatiefraude worden gepleegd, en vier casestudies: Nederland, Australië, Duitsland en Zweden. De casestudies zijn gebaseerd op bureauonderzoek en interviews met experts die beschikken over specialistische

[1] Tweede Kamer der Staten-Generaal (2026).

[2] NCTV (2025).

[3] NCTV (2025).

kennis rond kennisveiligheid, identiteitscontrole en documentverificatie. Door de ervaringen, werkwijzen en uitdagingen in deze landen te vergelijken, zijn relevante lessen geïdentificeerd voor Nederland. Interviews zijn ingezet om ontbrekende informatie aan te vullen en inzicht te geven in de praktijk.

Bevindingen

Wat is bekend over de wijze waarop identiteits- en documentatiefraude wordt gepleegd om toegang te krijgen tot kennisinstellingen in Nederland en daarbuiten?

Informatie over fraude met betrekking tot kennisveiligheid in Nederland wordt niet centraal geregistreerd of geanalyseerd. De verschillende actoren zijn door deze gefaseerde aanpak slechts in staat om een deel van het fraudebeeld te schetsen. In de interviews komen verschillende modus operandi van fraude aan bod. Het Loket Kennisveiligheid hoort regelmatig van kennisinstellingen dat informatie over bijvoorbeeld defensiegerelateerde banden bewust wordt weggelaten uit cv's. Dit gebeurt mede door de toegenomen aandacht voor kennisveiligheid en het groeiende bewustzijn bij kennisinstellingen van de risico's die bepaalde connecties met zich meebrengen. Waar dergelijke banden voorheen als prestigieus werden gezien, zijn instellingen zich nu meer bewust van de mogelijke risico's en de rol van statelijke actoren. Nuffic, de organisatie voor internationalisering in het onderwijs, adviseert Nederlandse kennisinstellingen over de waardering van buitenlandse diploma's en verstrekt jaarlijks circa 30.000 niet-bindende adviezen. Daarbij controleert Nuffic de authenticiteit en erkenning van diploma's door de bevoegde autoriteit en beoordeelt ze bijbehorende documenten zoals cijferlijsten. Door te toetsen of het gehele opleidingstraject logisch en consistent is verlopen, kan Nuffic mogelijke fraude opsporen. Omdat gebruik wordt gemaakt van kopieën kan het echter lastiger zijn om fraude vast te stellen, zeker als er statelijke actoren bij betrokken zijn. Nuffic signaleert dat fraude met diploma's vaker voorkomt uit bepaalde landen, maar onderzoekt niet expliciet of er een link is met kennisveiligheid. Daarnaast bestaan er bekende *diploma mills* – of diplomafabrieken – waar valse diploma's kunnen worden besteld.

In Australië zijn regelgevingsmechanismen zoals de PACT-voorschriften (*Protecting Australia's Critical Technology*) en het ARC-kader (Australian Research Council) ontworpen om grondige controles van documenten en bewijsstukken uit te voeren. Echter ligt de primaire focus daarbij niet op het opsporen van fraude en het verifiëren van de authenticiteit van documenten zoals identiteitsbewijzen en diploma's, maar veeleer op het identificeren van potentiële risico's. Uit interviews met Australische experts komt naar voren dat het geven van onjuiste informatie de belangrijkste vorm van fraude is die in Australië wordt aangetroffen, met name in cv's en subsidieaanvragen. Een van de meest zorgwekkende trends die zich de afgelopen twaalf tot achttien maanden heeft afgetekend, is het opzettelijk achterhouden van de herkomst van studiebeurzen. Er is sprake van een toenemende, systematische verkeerde voorstelling van financiering en van gevallen waarin personen opzettelijk aangeven banden te hebben met instellingen met een lager risico en hun banden met de daadwerkelijke (en mogelijk risicovollere) organisaties verzwijgen. Op cv's laten personen vaak bepaalde banen of stages weg in de officiële versies die zij indienen, en bewaren zij de volledige details voor cv's die privé worden gedeeld. Hetzelfde patroon is waarneembaar bij onderzoeksresultaten: onderzoek zonder *dual use* wordt openbaar gemaakt, terwijl militair gerelateerd onderzoek wordt verborgen. Bovendien worden affiliaties met organisaties vaak niet vertaald, waardoor hun werkelijke betekenis nog verder wordt achtergehouden. Een andere vastgestelde vorm van fraude betrof zijn valse uitnodigingsbrieven voor

visumdoeleinden. Vaak worden gevallen gesignaleerd door andere instellingen voor hoger onderwijs die contact opnemen om te bevestigen dat een uitnodiging authentiek is. Deze informatie-uitwisseling wordt mogelijk gemaakt door het Australische Informal Foreign Interference Network (INFIN), een niet-gouvernementele organisatie van 39 Australische instellingen voor hoger onderwijs die gezamenlijk de inspanningen tegen ongewenste inmenging en de naleving van overheidsvoorschriften bespreken.

In Duitsland ligt de verantwoordelijkheid voor screening bij de onderzoekers en universiteiten zelf. De wettelijke verplichtingen beperken zich tot exportcontroles op militaire en dual-use-technologieën. Instellingen moeten zelf informatie verzamelen over veiligheidsrelevante aspecten, vaak met behulp van externe bronnen zoals de ASPI-tracker, een tracker van het Australian Strategic Policy Institute (ASPI) die defensielinks van Chinese universiteiten in kaart brengt, maar die bieden beperkte en soms onduidelijke informatie. De Duitse binnenlandse veiligheidsdienst (Bundesamt für Verfassungsschutz – BfV) geeft wel een overzicht van methoden die risicovolle landen inzetten om gevoelige technologieën en kennis te vergaren, waarvan het ontwijken van export- en kenniscontrole door misleidende informatie in aanvragen te gebruiken direct relevant is voor kennisveiligheid. Dit komt overeen met trends in andere landen.[4]

Zweden hanteert een gecentraliseerd aanmeldingssysteem voor het hoger onderwijs dat beheerd wordt door de Zweedse Raad voor Hoger Onderwijs (UHR). UHR adviseert en biedt referenties, maar universiteiten en hogescholen beslissen zelf over toelating en zijn verantwoordelijk voor het controleren van kwalificaties en het opsporen van fraude. Bij PhD-aanmeldingen ligt deze verantwoordelijkheid volledig bij de instellingen zelf. Er is geen centrale rapportageplicht, waardoor de UHR geen inzicht heeft in het aantal fraudegevallen bij de instellingen. In een interview werd benoemd dat kandidaten met vervalste diploma's van diploma mills – instanties en personen die zich bezighouden met de verkoop van diploma's en academische graden zonder dat er een studieprogramma is gevolgd – zijn toegelaten tot PhD-programma's, wat de ernst van de kwestie onderstreept. Diploma mills vormen een groeiende uitdaging.

In het Verenigd Koninkrijk is er ook aandacht voor het achterhouden van informatie. Binnen ATAS (Academic Technology Approval Scheme) wordt niet alleen gekeken naar de inhoud van een aanvraag, maar ook naar mogelijke omissies, zoals hiaten in cv's. De aangeleverde documenten worden vergeleken met open-source-informatie en als bepaalde zaken niet worden genoemd, kan dit aanleiding zijn voor verder onderzoek.

Samenvattend lijken de belangrijkste modus operandi wat betreft identiteits- en documentatiefraude in de context van kennisveiligheid:

- Het gebruik van onvolledige documenten en het bewust achterhouden van informatie, bijvoorbeeld over affiliaties of herkomst van financiering;
- Het verdraaien of geven van onjuiste informatie, door bijvoorbeeld minder risicovolle affiliaties te vermelden. Het niet vertalen van dergelijke affiliaties kan het moeilijker maken om de werkelijke betekenis te achterhalen;
- Valse diploma's, bijvoorbeeld gefabriceerd door diploma mills;
- Valse uitnodigingsbrieven voor visumdoeleinden.

[4] Bundesamt für Verfassungsschutz (2026).

In hoeverre is er een beeld van de frequentie waarin deze fraude plaatsvindt in Nederland en daarbuiten?

Uit het literatuuronderzoek en de interviews is gebleken dat het zeer lastig is om een goed beeld te krijgen van de frequentie waarin deze fraude plaatsvindt in Nederland. Dit komt met name doordat sprake is van een gedecentraliseerd systeem, waarbij de verantwoordelijkheid voor de screening grotendeels bij de kennisinstellingen zelf ligt. Verschillende instanties controleren onderdelen van het proces, zoals de authenticiteit van diploma's, en hebben daardoor soms zicht op fraude binnen hun eigen domein. Zij geven echter aan geen volledig overzicht te hebben. Zo heeft Nuffic een adviserende rol, maar zijn universiteiten niet verplicht diploma's door Nuffic te laten controleren.

Volgens geïnterviewde experts in Australië zijn er tot op heden geen gevallen ontdekt van personen die onder een valse identiteit reisden. Zij voegen hieraan toe dat – aangezien buitenlandse staatsactoren de grootste bedreiging vormen – het wellicht onmogelijk is om frauduleuze referenties op te sporen wanneer deze door overheidsinstanties zijn uitgegeven. Zoals eerder aangegeven is de belangrijkste vorm van fraude in Australië het geven van onjuiste informatie, met name in cv's en subsidieaanvragen. Ook van de omvang van dit fenomeen bestaat geen compleet beeld. Dat het gebeurt is echter duidelijk: de China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië en toch gaven slechts 350 studenten openlijk toe deze steun te ontvangen. Deze aanzienlijke discrepantie onderstreept hoe vaak personen niet transparant zijn over de aard of de bron van hun onderzoeksfinanciering. Omdat het hierbij gaat om een enkele bron van financiering, is dit mogelijk slechts het topje van de ijsberg van een groter probleem waarbij ook andere informatie wordt achtergehouden. Wat betreft valse uitnodigingsbrieven voor visumdoeleinden registreerde de Australische universiteit van New South Wales in de afgelopen twee tot drie jaar 6 tot 12 gevallen. Dit komt voornamelijk voor op faculteitsniveau, bij gastwetenschappers. Opvallend is dat er geen relevante casestudies zijn met betrekking tot de PACT-voorschriften. Hoewel het PACT-mechanisme is toegepast om visumaanvragen te beperken, blijven beslissingen hierover buiten het publieke domein. Tijdens een interview wordt opgemerkt dat deze alleen openbaar worden gemaakt als een aanvrager in de toekomst besluit een beslissing aan te vechten.

Net als in Duitsland, ligt ook in Zweden de verantwoordelijkheid bij de kennisinstellingen zelf, waardoor het eveneens in dit land lastig is om een beeld te krijgen van de frequentie. Wel worden toelatingen van bachelor- en masterstudenten gecentraliseerd bij de UHR behandeld. Uit een interview kwam naar voren dat voor academische toelatingen via het UHR-portaal het aantal gemelde fraudegevallen is gestegen, van 30 in 2024 tot 130 in 2025. Dit wordt grotendeels toegeschreven aan het gebruik van AI-agenten waardoor de aanmeldingsprocedure toegankelijker zou zijn geworden. Hier is echter geen directe link met kennisveiligheid te maken, want het kan bijvoorbeeld ook gaan om fraude om economische migratiedoeleinden. De aantallen geven echter wel een beeld van de schaal en de mogelijk groeiende rol van AI.

Welke waarborgen kunnen worden gecreëerd om de verschillende vormen van fraude tegen te gaan?

Uit het literatuuronderzoek en de interviews komen meerdere lessen voor Nederland naar voren, dan wel waarborgen die kunnen worden gecreëerd om de verschillende vormen van fraude tegen te gaan.

Screening op individueel en institutioneel-/landenniveau beter samenbrengen

Interviews en praktijkervaringen laten zien dat het opsporen van inconsistenties essentieel is voor het signaleren van fraude, vooral bij het gebruik van kopieën of de betrokkenheid van statelijke actoren.[5] Uit een interview voor de casestudie over Zweden bleek bijvoorbeeld dat het verifiëren van publicaties een van de voornaamste manieren is waarop ze controleren op mogelijke defensielinks.[6] Ook kunnen publicaties worden vergeleken met informatie op een cv waardoor inconsistenties aan het licht kunnen komen.[7] In Nederland ontvangt het Loket Kennisveiligheid, het centraal adviespunt voor kennisinstellingen, geen persoonsgegevens. Individuele screening ligt bij de kennisinstellingen, die hiervoor vaak beperkte middelen en landenkennis hebben. Een volledig beeld is daarom afhankelijk van vrijwillige coördinatie en kennisdeling tussen instanties. In bijvoorbeeld Frankrijk komt kennis over risico's op individueel en institutioneel-/landenniveau meer samen, doordat de kennisveiligheidscoördinator binnen kennisinstellingen een vertrouwelijke functie heeft en wordt aangesteld door de overheid.

Verken informatievoorziening voor kennisinstellingen over kennisdeling

Controles ten behoeve van kennisveiligheid zijn in alle onderzochte landen versnipperd over meerdere instanties. Dit wordt verder gecompliceerd doordat de benodigde informatie doorgaans persoonsgegevens omvat, en het delen ervan secuur en in overeenstemming met privacywetgeving moet gebeuren. In Zweden wordt dit bijvoorbeeld als heikel punt ervaren. Zelfs als fraude wordt vastgesteld tijdens een toelatingsprocedure kan deze informatie vaak niet extern, of zelfs niet intern, gedeeld worden.[8] In Zweden geeft de UHR zowel erkenning met het oog op de arbeidsmarkt als met het oog op vervolgstudies. Vanwege de regels rond gegevensbescherming is het delen van informatie tussen de twee procedures verboden, zelfs wanneer een persoon voor beide doeleinden een aanvraag heeft ingediend.[9] In Nederland geven betrokken instanties zoals Nuffic adviezen, maar zijn kennisinstellingen niet verplicht om advies in te winnen en behouden ze altijd de bevoegdheid om zelf te beslissen over toelating. Hierdoor kan het voorkomen dat een student, voor wie Nuffic zich heeft onthouden van advies vanwege twijfels over de authenticiteit of erkenning van documenten, bij de ene instelling niet wordt toegelaten, maar elders wel. In de praktijk vragen kennisinstellingen voor bepaalde herkomstlanden vrijwel altijd advies aan, maar ligt de interpretatie en uiteindelijke beslissing bij de instelling zelf.[10] Uit eerder onderzoek bleek al dat kennisinstellingen het zonder duidelijke wettelijke kaders lastig vinden om in te schatten wat ze AVG-technisch mogen opvragen en wie ze wel en niet moeten toetsen.[11] Kennisinstellingen hebben behoefte aan heldere richtlijnen en praktische ondersteuning over wat zij op grond van privacywetgeving mogen opvragen, wie zij wel of niet moeten screenen en hoe persoonsgegevens gedeeld mogen worden. Ook is er behoefte aan duidelijke richtlijnen over wanneer en op welke wijze fraudegevallen moeten worden opgeschaald of doorgezet naar andere instanties, zoals de inlichtingendiensten.

[5] RAND Europe Interview – 8.

[6] RAND Europe Interview – 9.

[7] RAND Europe Interview – 4.

[8] RAND Europe Interview – 14.

[9] RAND Europe Interview – 14.

[10] RAND Europe Interview – 8.

[11] Bokdam et al. (2023).

Organiseer herhaalde en gelaagde screening

In veel landen, zoals Australië, zijn formele controles ingebouwd in het visum- of financieringsproces, waardoor meerdere instanties betrokken zijn bij de screening. In Zweden en Duitsland zijn overheidsinstanties verantwoordelijk voor visumcontroles. In Nederland is het systeem gebaseerd op de Wet modern migratiebeleid (wet MoMi), waarbij kennisinstellingen als erkende referenten optreden en een belangrijke verantwoordelijkheid dragen voor het indienen en onderbouwen van aanvragen. De formele beoordeling van en beslissing op aanvragen blijft bij de IND. Het systeem gaat daarbij uit van een vertrouwensrelatie tussen de overheid en de erkende referent, waarbij controles mede op basis van signalen en achteraf steekproefsgewijs plaatsvinden.[12] Hierdoor speelt de kennisinstelling een belangrijke rol in het toelatingsproces, terwijl in andere landen de overheid een grotere rol speelt bij het visumproces. Effectieve kennisveiligheid vraagt om gelaagde screening, waarbij zowel overheidsinstanties als kennisinstellingen een actieve rol spelen gedurende het hele traject.

Zet technische expertise in bij screening

Het Britse systeem legt een sterke nadruk op technische expertise en duiding. Dit is essentieel, omdat ambtenaren vaak niet over de benodigde kennis van sensitieve vakgebieden beschikken. Het is belangrijk om experts te hebben die inzicht hebben in de risico's en die hun kennis voortdurend op peil houden, gezien de snelle veranderingen binnen de wetenschap.[13] Het belang van technische expertise en duiding komt ook in Frankrijk naar voren.[14] Daar krijgen onderzoekers een ambtelijke aanstelling, waardoor het makkelijker is om zowel ambtenaar als onderzoeker te zijn of tussen de functies te wisselen. Zo worden wetenschappers direct onderdeel van het screeningsproces.[15] De belangrijkste les is dat effectieve kennisveiligheid vraagt om structurele samenwerking tussen ambtenaren, kennisveiligheidscoördinatoren en wetenschappelijke experts, zodat technische en strategische duiding altijd beschikbaar is bij de beoordeling van risico's. Het opzetten van vaste overlegstructuren of expertgroepen, kan hierbij als *best practice* dienen.

Coördineer informatieverstrekking en landenkennis om fraude te herkennen

Een van de belangrijkste lessen uit dit onderzoek is het belang van het verkrijgen van de juiste informatie en het hebben van (landen)kennis en data om deze juist te interpreteren. Wat duidelijk werd uit meerdere casestudies is dat een van de meest gesignaleerde vormen van fraude het achterhouden of verdraaien van informatie is, waardoor bijvoorbeeld defensielinks niet zichtbaar worden. Het Loket Kennisveiligheid krijgt regelmatig vragen van kennisinstellingen over buitenlandse entiteiten die van naam veranderen of fuseren met andere instituten, wat het lastiger maakt om ze te volgen.[16] Ook het achterhouden van bepaalde financiering is gangbaar, zoals bleek uit de Australische casestudie. De China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië, maar bij hun aanmelding gaven slechts 350 studenten openlijk toe deze steun te ontvangen.[17]

[12] Lodder (2019).

[13] RAND Europe Interview – 2.

[14] RAND Europe Interview – 2.

[15] RAND Europe Interview – 2.

[16] RAND Europe Interview – 4.

[17] RAND Europe Interview – 7.

Landenkennis

Een belangrijke waarborg voor een effectieve kennisveiligheidsscreening is het beschikken over specifieke landenkennis, zodat aangeleverde documenten en informatie correct kunnen worden geïnterpreteerd. Het Loket Kennisveiligheid heeft bijvoorbeeld medewerkers met kennis van relevante talen en culturele context die risico's beter kunnen inschatten. Inzicht in financieringsbronnen uit risicolanden maakt het mogelijk om te beoordelen of er sprake is van financiering met mogelijke defensielinks. Daarnaast maakt deze expertise het eenvoudiger om ontwikkelingen bij buitenlandse entiteiten, zoals naamswijzigingen, te volgen. Landenspecialisatie draagt bovendien bij aan het herkennen van terugkerende fraudepatronen, zoals ook uit interviews met Nuffic en hun Zweedse tegenhanger blijkt. Daar werken landenspecialisten die door hun ervaring snel patronen in fraude kunnen identificeren.

Goed begrip van en data over risicoindicatoren

In meerdere interviews komt naar voren dat tijdens het screeningsproces veelvuldig gebruik wordt gemaakt van de ASPI-tracker. Dergelijke instrumenten kunnen helpen om de informatie die wordt aangeleverd tijdens een aanmelding juist te interpreteren en zo bepaalde risico's tegen te gaan, zoals het gebruik van historische institutionele namen of acroniemen. Advies vanuit de overheid, afstemming tussen risicoindicatoren en tools om hierop te checken zouden welkom zijn, zodat kennisinstellingen dezelfde afwegingen maken.[18] De Europese Commissie werkt aan de ontwikkeling van een beveiligd IT-platform dat betrouwbare informatie over buitenlandse onderzoeksinstellingen zal verzamelen om onderzoekers te helpen inzicht te krijgen in de mogelijke risico's die gepaard gaan met het aannemen van buitenlandse onderzoekers.[19] Het is wenselijk dat kennisinstellingen actief participeren in de ontwikkeling en het gebruik van het Europese due-diligence-platform. Door ervaringen en best practices te delen, kan het platform optimaal aansluiten bij de behoeften van de praktijk.

Disclosure-voorwaarden

In Australië gelden in het ARC-proces bijvoorbeeld zogenoemde disclosure-voorwaarden voor risicoindicatoren, waarbij onderzoekers met niet-Australische affiliaties hun financiering en deelname aan talentprogramma's verplicht moeten melden.[20] Het ARC Research Security Framework bepaalt welke informatie verstrekt moet worden en legt de controle bij de universiteiten. Deze centrale disclosure-eisen geven kennisinstellingen helderheid over welke informatie zij moeten opvragen en zorgen voor een systematische aanpak. Hierdoor kan fraude, zoals het achterhouden van financiering door de China Scholarship Council, beter worden vastgesteld en zijn de consequenties van het niet melden vooraf duidelijk. Het invoeren van vergelijkbare, centraal vastgelegde disclosure-voorwaarden kan bijdragen aan meer transparantie en een eerlijk speelveld.

Zorg voor Europese coördinatie om weglekken te voorkomen

Het Loket Kennisveiligheid hoort regelmatig van kennisinstellingen dat er behoefte is aan een gelijker speelveld binnen Europa. Er bestaat concurrentie tussen Europese universiteiten, waardoor het problematisch is als in Nederland bepaald onderzoek wordt gehinderd vanwege veiligheidsrisico's rond

[18] Bokdam et al. (2023).

[19] European Union (2026).

[20] Australian Research Council (2026a)

buitenlandse onderzoekers, terwijl universiteiten in andere landen dergelijke onderzoekers ongehinderd toelaten. Dit kan Nederlandse instellingen op achterstand zetten.[21] Ook werken Nederlandse kennisinstellingen nauw samen met omliggende landen, waardoor sensitieve kennis en technologie alsnog kunnen weglekken.[22]

[21] RAND Europe Interview – 4.

[22] European Union (2026).