Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek

Sectorbeeld onderzoeksinstituten KNAW en NWO-I

Johan Bokdam, Anne Wester (Oberon), Max Kemman, Timon de Boer, Femke van Wijk en José van der Geest (Dialogic)

dialogic
innovatie • interactie

Oberon
onderzoek | advies

Inhoudsopgave

Samenvatting **5**

1 Inleiding **9**
1.1 Achtergrond van het onderzoek 9
1.2 Doel en vraagstelling 10
1.3 Onderzoeksopzet 10

2 Afbakening en ontwikkeling kennisveiligheidsbeleid **13**
2.1 Afbakening kennisveiligheid en diversiteit in de sector 13
2.2 Ontwikkeling van kennisveiligheidsbeleid 14

3 Risicoanalyses **16**
3.1 Risicoanalyse 2022 16
3.2 Risicoanalyse als onderdeel van het kennisveiligheidsbeleid 18
3.3 Dilemma's en aandachtpunten 19
3.4 Lessons learned 19

4 Risicomanagement en fysieke en digitale maatregelen **20**
4.1 Organisatie risicomanagement 20
4.2 Fysieke en digitale beschermingsmaatregelen 24
4.3 Dilemma's en aandachtspunten 26
4.4 Lessons learned 26

5 Internationale partnerschappen en juridische kaders **28**
5.1 Internationale partnerschappen 28
5.2 Juridische kaders en gedragscodes 30
5.3 Dilemma's en aandachtspunten 32
5.4 Lessons learned 32

6 Personeelsbeleid **33**
6.1 Vertaling kennisveiligheid in personeelsbeleid 33
6.2 Dilemma's en aandachtspunten 35
6.3 Lessons learned 36

7 Conclusie en aandachtspunten **37**
7.1 Conclusie: beleid in ontwikkeling, betrokkenen zien beperkt risico's 37
7.2 Dilemma's 39
7.3 Aandachtspunt 40

Bijlage 1 Vragenlijst **41**

Samenvatting

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft onderzoeksbureaus Oberon en Dialogic gevraagd onderzoek te doen naar het kennisveiligheidsbeleid van kennisinstellingen. Dit sectorbeeld beschrijft de uitkomsten van dit onderzoek voor de KNAW- en NWO-instituten. Eerder zijn de sectorbeelden voor de universiteiten[1] en hogescholen[2] verschenen.

Achtergrond, doel en aanpak
Dit sectorbeeld brengt in kaart waar de KNAW, NWO-I en hun instituten eind 2023 staan met de uitwerking van kennisveiligheidsbeleid, welke uitdagingen zij daarbij zien en hoe zij hiermee omgaan. Daarbij kijken we naar de wijze waarop en de mate waarin de Nationale Leidraad Kennisveiligheid (de Leidraad) is vertaald in instellingsbeleid en de manier waarop de KNAW en NWO-I opvolging hebben gegeven aan de oproep van de minister in april 2022 om een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren. Het onderzoek is van eind 2023 tot begin 2024 uitgevoerd middels een begeleide self-assessment onder 9 KNAW-instituten en 9 NWO-instituten en de bureaus van KNAW en NWO-I. Dit beeld is daarna verdiept met een casestudy. Hieronder vatten we de stand van zaken samen aan de hand van de hoofdstukken uit de Leidraad.

Afbakening kennisveiligheidsbeleid
De Leidraad definieert kennisveiligheid als “het voorkomen van ongewenste overdracht van sensitieve kennis en technologie met negatieve gevolgen voor onze nationale veiligheid en de Nederlandse innovatiekracht. Daarnaast gaat het om heimelijke beïnvloedings- en inmengingsactiviteiten van statelijke actoren in hoger onderwijs en wetenschap. Dergelijke beïnvloeding (*foreign interference*) kan leiden tot vormen van (zelf)censuur resulterend in aantasting van de academische vrijheid. Tot slot draait het bij kennisveiligheid om ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd.” In dit rapport schrijven we in het kort over ongewenste overdracht van sensitieve kennis en technologie, heimelijke beïnvloeding en ethische kwesties als de onderwerpen van kennisveiligheid.
De definitie en afbakening van kennisveiligheid en beleid wordt door de beide bureaus gecoördineerd en geharmoniseerd. Zowel de KNAW als NWO-I vertrekken vanuit de definitie van kennisveiligheid van de Leidraad, met primair aandacht voor ongewenste overdracht van sensitieve kennis en technologie. Daarbij ligt de aandacht voornamelijk op nationale veiligheid (onder meer *dual use*) en minder op innovatiekracht of economische veiligheid.

Beleid in ontwikkeling, betrokkenen zien beperkt risico’s
Het belang van het kennisveiligheidsbeleid is bij zowel KNAW als NWO-I in een stroomversnelling geraakt door de oproep van de minister. De beleidsontwikkeling en vaststelling ligt bij de bureaus, en de implementatie en instituut-specifieke invulling ligt bij de instituten. Het belang van kennisveiligheidsbeleid wordt door de diverse instituten verschillend ervaren, waarbij de bureaus en instituten over het algemeen beperkt risico’s zien op het vlak van kennisveiligheid.
De instituten zijn meestal beperkt in omvang, variërend van enkele tientallen tot enkele honderden medewerkers, met een overzichtelijk aantal onderzoeksgroepleiders. Hierdoor weten betrokkenen bij kennisveiligheid elkaar goed te vinden. Men is snel bekend met casuïstiek en het persoonlijke contact helpt om vervolgens op een goede manier daarmee om te gaan. Waar de bureaus toezien op het

[1] Sectorbeeld kennisveiligheid universiteiten 2023 | Rapport | Rijksoverheid.nl
[2] Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek - Sectorbeeld hogescholen | Rapport | Rijksoverheid.nl

vaststellen van formeel beleid, kiezen veel instituten er daarom voor om op instituutsniveau het beleid op meer informele wijze te implementeren. Doordat de instituten beperkt van omvang zijn, vindt er veel samenwerking plaats tussen instituten en de bureaus op kennisveiligheidsbeleid. In beide organisaties zijn adviesteams ingericht die worden ondersteund door de coördinator kennisveiligheid van het desbetreffende bureau.

Veel NWO-instituten voeren technologisch onderzoek uit, zijn al langer bewust van de gevoeligheid van hun onderzoeksgebied en voeren hier beleid op. Een nuancering die zij daarbij geven is dat zij voornamelijk fundamenteel onderzoek uitvoeren, waardoor er geen directe toepassingsrisico's zijn. Er is veel samenwerking en afstemming tussen de NWO-instituten en de ondersteuning vanuit het NWO-I-bureau is vrij intensief. Er is dus ruime aandacht voor kennisveiligheid, hoewel dit als arbeidsintensief wordt ervaren. De KNAW-instituten zijn vaker gericht op sociaal- of geesteswetenschappelijk onderzoek, waar sensitieve technologie en exportbeperkingen niet spelen. Meerdere instituten geven aan dat zij daarom beperkt te maken hebben met kennisveiligheidsvraagstukken. Dit is opvallend, omdat de KNAW in een *position paper* eerder adviseerde "differentieer steeds tussen de drie verschillende betekenissen van 'kennisveiligheid'."[3] Enkele instituten geven aan dat zij vooral risico's zien op ongewenst gebruik van hun data, waar ze op inspelen met hun beleid op informatiebeveiliging.

De KNAW- en NWO-instituten hebben zelf per onderdeel van de Leidraad hun fase van beleidsontwikkeling gescoord. Onderstaande tabel brengt een aantal verschillen naar voren:

- Beleid op fysieke en digitale bescherming is vaker vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid.
- Beleid op (risicovolle) internationale partnerschappen is bij de KNAW en NWO-I op het niveau van de bureaus vastgesteld met aantoonbare uitvoering. Daarnaast is de implementatie van het beleid uitgevraagd bij de NWO-instituten; zij zitten in verschillende fases van beleidsimplementatie.
- Beleid voor toepassing van juridische kaders (zoals compliance met export controle en sanctieregimes) ontbreekt relatief vaker dan de andere onderdelen in het kennisveiligheidsbeleid.
- De vertaling van kennisveiligheid in het personeelsbeleid is bij de meerderheid van de instituten vastgesteld met aantoonbare uitvoering.

Tabel S.1 Zelfscores op fase van beleidsontwikkeling. (een aantal instituten heeft op één of meer onderdelen geen score ingevuld. Hierdoor verschilt de n per onderwerp)

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en uitvoering	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig
Risicoanalyses	1	6	6	3	2	
Risicomanagement	1	6	3	5	1	2
Fysieke en digitale beschermingsmaatregelen	1	2	2	9	2	2
Internationale partnerschappen (NWO-instituten)	1	2	2	2		
Juridische kaders	7	1		5	1	
Personeelsbeleid	3	3	2	7		3

[3] KNAW (2023). Kennisveiligheid - KNAW position paper, p. 2.

Risicoanalyse 2022
De minister van OCW heeft in 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren. Vrijwel alle KNAW- en NWO-instituten (16 van de 18) hebben hierop een risicoanalyse uitgevoerd. Twee instituten geven aan dat ze geen eigen risicoanalyse hebben uitgevoerd op instituutsniveau, omdat ze dit minder relevant achtten voor het type samenwerkingen of onderzoek dat wordt uitgevoerd. Eén van deze twee heeft dit wel voor enkele projecten gedaan.
Voor de helft van de instituten (9 van de 18) was dit de eerste keer dat ze een risicoanalyse op kennisveiligheid uitvoerden. Drie instituten hebben op basis van de risicoanalyse nieuwe risico's geïdentificeerd. De bureaus geven verder aan dat de risicoanalyses tot meer inzicht in en bewustwording van de risico's bij de verschillende instituten hebben geleid.

Risicomanagement en fysieke en digitale maatregelen
De KNAW- en NWO-I-bureaus hebben een bestuurlijk portefeuillehouder kennisveiligheid. Bij het KNAW-bureau valt deze portefeuille onder de taken van de president. Bij NWO-I ligt de portefeuille bij een van de leden van het stichtingsbestuur van NWO-I en bij een van de instituutsdirecteuren. Beide bureaus hebben op centraal niveau een Adviesteam Kennisveiligheid ingesteld. Daarnaast staat kennisveiligheid op de agenda van verschillende overleggen tussen instituten, zoals reguliere vergaderingen van instituutsdirecteuren, van instituutsmanagers of van bedrijfsvoerders.

Een essentieel onderdeel van kennisveiligheidsbeleid is het vergroten van het bewustzijn hierover onder het personeel. Onderzoekers als inhoudelijk experts zijn noodzakelijk voor het signaleren van kennisveiligheidsrisico's en worden meegenomen in het risicomanagement. De helft van de instituten (9 van de 18) geeft aan bewustwordingscampagnes te voeren rondom kennisveiligheid. De KNAW en NWO-I hebben hiervoor beiden een campagne ontwikkeld. Bij de KNAW staat de campagne voor 2024 op de planning, bij NWO-I wordt deze al toegepast. Deze bewustwordingscampagnes zijn gericht op alle onderzoekers in alle lagen van de instituten. Daarnaast krijg kennisveiligheid in de managementoverleggen met groepsleiders en senior personeel aandacht, met het idee dat deze bewustwording doorstroomt naar de andere medewerkers van de teams.

Het merendeel van de instituten (16 van de 18) heeft een restrictief toegangsbeleid voor bepaalde ruimtes (zoals afdelingen, gebouwen of labs). Twee instituten geven aan dat restrictief toegangsbeleid niet relevant is, bijvoorbeeld omdat het instituut geen ruimtes heeft waar dit nodig is. Ook geeft het merendeel van de instituten (16 van de 18) aan dat ze beleid hebben omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten. Meermaals wordt aangegeven dat dit beleid zich meer richt op omgang met gevoelige persoonsgegevens en informatieveiligheid (o.a. omtrent patenten) dan op kennisveiligheidsrisico's.

Internationale partnerschappen en juridische kaders
Het KNAW-bureau zal in 2024 een centraal overzicht van risicovolle partnerschappen voor alle instituten ontwikkelen. Bij twee NWO-instituten is een centraal overzicht van veiligheidsgevoelige partnerschappen aanwezig, bij de overige zeven NWO-instituten en het centrale NWO-I-bureau is zo'n overzicht ook gepland voor 2024. NWO-instituten werken maar weinig samen met partners uit risicovolle landen, waardoor een dergelijk overzicht later is gepland. Het uitvoeren van *due diligence* voor het aangaan van internationale partnerschappen ligt bij zowel de KNAW als NWO-I bij de bureaus. Bij zowel de KNAW als NWO-I ligt de besluitvorming over risicovolle partnerschappen op centraal bestuurlijk niveau bij respectievelijk de KNAW-directie en de NWO-I-portefeuillehouder.

Personeelsbeleid
De meerderheid van de instituten (15 van de 18) ontwikkelt of heeft al aandacht voor kennisveiligheid als onderdeel van het personeelsbeleid. 12 van de 18 instituten geven aan in meer of mindere mate veiligheidsrisico's mee te wegen bij de werving en selectie van nieuwe medewerkers. Deze instituten voeren cv-checks uit, vragen advies aan het Loket Kennisveiligheid, vragen om een Verklaring Omtrent het Gedrag (VOG) of voeren zelf een (globale) check uit op connecties met landen met een verhoogd risicoprofiel. 17 van de 18 instituten hebben geen specifiek beleid om te voorkomen dat de sociale veiligheid wordt aangetast door (heimelijke) beïnvloeding. Een aantal van hen licht toe dat beïnvloeding door statelijke actoren van hun medewerkers niet lijkt voor te komen, omdat zij niet samenwerken met landen met een verhoogd risicoprofiel en/of omdat er geen medewerkers uit landen met een verhoogd risicoprofiel bij het instituut werken. Eén instituut heeft als beleid persoonlijke gesprekken te houden met medewerkers uit landen met een verhoogd risicoprofiel die betrokken zijn bij onderzoek dat valt onder de kroonjuwelen.

Dilemma's en aandachtspunten ten aanzien van het kennisveiligheidsbeleid
In het ontwikkelen en uitvoeren van kennisveiligheidsbeleid zien we een aantal algemene dilemma's, zorgen en aandachtspunten bij de instituten die van belang zijn voor het debat over kennisveiligheidsbeleid:

- Een belangrijke zorg is **het voorkomen van stigmatisering en discriminatie**, of een cultuur van uitsluiting op terreinen waar er geen duidelijke sancties of juridische kaders zijn. Abstract nationaal beleid vertaalt zich binnen de instellingen tot impact op het individuele niveau van veelbelovende sollicitanten en gewaardeerde collega's.
- Het kennisveiligheidsbeleid is in sterke mate gericht op **technologisch onderzoek**, met veel aandacht voor het voorkomen van ongewenste overdacht van sensitieve kennis en technologie. Meerdere instituten geven aan dat ze een **laag risicoprofiel** hebben, omdat ze actief zijn op niet-sensitieve kennisgebieden of omdat technologisch onderzoek op het laagste TRL-niveau plaatsvindt. De relevantie en proportionaliteit van kennisveiligheidsbeleid is daarom punt van discussie.
- Kennisveiligheidsbeleid vraagt om een **nieuwe balans** tussen **academische waarden en nationale veiligheid**. Wetenschappelijk onderzoek is sterk gericht op kennisdeling en internationale samenwerking en kent traditioneel weinig structuren om kennis juist te beschermen. De structuren, culturen en motivaties vanuit deze twee opvattingen botsen in de praktijk.
- Risicoanalyses zijn in sterke mate gericht op het eigen risicoprofiel van kennisgebieden, faciliteiten en medewerkers. Een vraag is echter in welke mate het *externe* risicoprofiel van instituten moet worden meegewogen. Sommige instituten doen zelf geen sensitief onderzoek, maar hebben wel een goede reputatie. Deze instituten geven aan dat hun ex-werknemers, dankzij een goede referentie, zeer makkelijk binnenkomen bij werkgevers waar mogelijk wel sensitief onderzoek wordt gedaan. Deze instituten fungeren daarmee als **toegangspoort tot andere organisaties of kennisinstellingen**.
- Vanuit het belang van een **internationaal gelijk speelveld** en het voorkomen van een internationaal waterbedeffect is er behoefte aan consistent en afgestemd nationaal en Europees beleid.
- **Conceptualisering van kennisveiligheid**. De KNAW en NWO-instituten hebben door het gebruik van de KWAS hun risicoanalyse in sterke mate gericht op het identificeren van kroonjuwelen. Over de definitie van wat kroonjuwelen zijn en hoe hier vervolgens kennisveiligheidsbeleid op te ontwikkelen zijn nog verschillen van inzicht. Het zou nuttig zijn om hier als overheid en sector gezamenlijk verder aan zowel conceptualisering als definiëring te werken, en dit te verwerken in een volgende editie van de Nationale Leidraad Kennisveiligheid of een aangepaste handreiking voor de analyses.

1 Inleiding

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft onderzoeksbureaus Oberon en Dialogic gevraagd onderzoek te doen naar het kennisveiligheidsbeleid van instellingen voor hoger onderwijs en onderzoek. Dit sectorbeeld beschrijft de uitkomsten van dit onderzoek voor de onderzoeksinstituten van de KNAW en NWO-I. Eerder verschenen sectorbeelden voor de universiteiten[4] en voor de hogescholen[5].

1.1 Achtergrond van het onderzoek

Op 31 januari 2022 hebben de Rijksoverheid en de Nederlandse kennissector, vertegenwoordigd door UNL, de VH, NFU, de TO2 federatie, KNAW en NWO, gezamenlijk de Nationale Leidraad Kennisveiligheid (hierna: de Leidraad) gepubliceerd.[6] Deze Leidraad is een richtinggevend referentiedocument voor alle kennisinstellingen van Nederland. Onderdeel van de Leidraad is de opdracht dat alle instellingen een risicoanalyse maken van internationale samenwerkingen en financieringsbronnen op sensitieve kennisgebieden.

De minister van OCW heeft in april 2022 alle kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren. In het bestuursakkoord 2022 hoger onderwijs en wetenschap hebben OCW, UNL en de VH afgesproken dat een externe audit zal plaatsvinden op de (mate van) implementatie van de Leidraad.[7] In de loop van 2023 hebben de KNAW en NWO-I in overleg met OCW besloten dat ook hun instituten deelnemen aan deze audit. In het spoeddebat kennisveiligheid was deze externe audit eerder toegezegd aan de Tweede Kamer.[8] In dat debat werd onderscheid gemaakt tussen een *inhoudelijke audit*, waarbij externe onderzoekers de samenwerkingsverbanden en specifieke aanstellingen beoordelen, en een *procesaudit*, waarbij externe onderzoekers nagaan hoe de Leidraad wordt opgevolgd.
Voor dit onderzoek is gekozen voor een procesevaluatie. Omdat kennisveiligheid als thema de laatste jaren aan urgentie heeft gewonnen en nog volop in ontwikkeling is, is er ook (nog) geen normenkader voor een inhoudelijke audit. Het Wetsvoorstel Screening Kennisveiligheid,[9] waarin moet worden uitgewerkt welke kennisgebieden als sensitief worden aangemerkt, is bijvoorbeeld nog in ontwikkeling. Ook is nog niet bekend of dit wetsvoorstel voldoende basis geeft voor een inhoudelijke audit. Daarnaast is sprake van een momentopname: de kern van het onderzoek is waar de kennisinstellingen in 2023 staan met hun kennisveiligheidsbeleid en hoe dit (verder) ontwikkeld wordt. We onderzoeken de stand van implementatie van de Leidraad en hoe opvolging is gegeven aan de oproep van de minister in 2022 om een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren.[10] Het onderzoek geeft op deze manier invulling aan de externe audit kennisveiligheid die de minister aan de Tweede Kamer heeft toegezegd. Ook is hiermee een opzet gekozen die kan dienen als basis voor vervolgmetingen,

4 Sectorbeeld kennisveiligheid universiteiten 2023 | Rapport | Rijksoverheid.nl
5 Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek - Sectorbeeld hogescholen | Rapport | Rijksoverheid.nl
6 Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken | Rapport | Rijksoverheid.nl
7 Bestuursakkoord 2022 hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl
8 Commissiedebat Hoger Onderwijs- Onderzoek- en Wetenschapsbeleid (23 juni 2022). *Spoeddebat kennisveiligheid.*
9 Kamerbrief inzake tijdpad wetstraject Screening Kennisveiligheid en uitwerking amendement middelen kennisveiligheidsbeleid | Kamerstuk | Rijksoverheid.nl
10 Zie: Afschrift brief aan kennisinstellingen Nationale Leidraad Kennisveiligheid | Brief | Rijksoverheid.nl

zodat komende jaren de ontwikkeling van het kennisveiligheidsbeleid op sectorniveau in kaart kan worden gebracht.

1.2 Doel en vraagstelling

Het doel van het onderzoek is om een beeld op te halen waar de kennisinstellingen staan met de uitwerking van hun kennisveiligheidsbeleid. In dit rapport beschrijven we de resultaten voor de KNAW- en NWO-instituten. We beschrijven die zo dat dit rapport zelfstandig leesbaar is zonder benodigde voorkennis van de andere sectorbeelden; om deze reden zijn sommige beschrijvingen uit de eerdere sectorbeelden herhaald.
In dit rapport wordt de wijze waarop en de mate waarin de Leidraad is vertaald in het instituutsbeleid en de manier waarop risicoanalyses op internationale samenwerkingen zijn uitgevoerd in beeld gebracht. Dit leidt tot de volgende centrale onderzoeksvraag: *Waar staan de onderzoeksinstituten van de KNAW en NWO-I met de uitwerking van het kennisveiligheidsbeleid?* Deze vraag splitsen we uit naar vier onderdelen die in hoofdstuk 3 tot en met 6 aan bod komen:

1 Risicoanalyses (en de risicoanalyse 2022).
2 Risicomanagement (inclusief fysieke en digitale maatregelen).
3 Internationale partnerschappen (inclusief juridische kaders).
4 Personeelsbeleid.

We volgen bovendien het advies van de AWTI voor een **lerende aanpak**.[11] In de beantwoording van de onderzoeksvraag geven we daarom niet alleen inzicht in de mate van uitwerking van het kennisveiligheidsbeleid. Ook besteden we aandacht aan dilemma's waarmee de KNAW- en NWO-instituten zich geconfronteerd zien en eventuele *lessons learned* waar zij van elkaar kunnen leren.

1.3 Onderzoeksopzet

Het onderzoek kent vier fases, waarin verschillende activiteiten zijn uitgevoerd. In Tabel 1.1. geven we een overzicht, dat daarna wordt toegelicht. De kern van het onderzoek is een **begeleide zelfevaluatie** door de instituten. De begeleiding bestond eruit dat KNAW en NWO-instituten vragenlijsten voorgelegd kregen die zij puntsgewijs dienden te beantwoorden. In het geval een vraag niet goed begrepen werd konden de KNAW en NWO-I contact opnemen met de onderzoekers.

1.3.1 Voorbereiding

De vragenlijst voor de begeleide zelfevaluatie is een aangepaste versie van de vragenlijst die eerder in 2023 is ontwikkeld en gebruikt voor universiteiten en hogescholen. Specifiek voor KNAW en NWO-I[12] geldt dat verschillende verantwoordelijkheden voor het kennisveiligheidsbeleid zijn verdeeld over de centrale bureaus en de zelfstandige onderzoeksinstituten. In overleg met de KNAW en NWO-I is de vragenlijst daarom opgedeeld in een deel met vragen voor de centrale bureaus en een deel met vragen voor de individuele onderzoeksinstituten. Omdat deze verdeling – en daarmee knip in de vragenlijst -

[11] AWTI (2022). Kennis in conflict. Veiligheid en vrijheid in balans.
[12] NWO-I of de Stichting Nederlandse Wetenschappelijk Onderzoek Instituten is een koepelorganisatie voor negen nationale onderzoeksinstituten. Het is een zelfstandige privaatrechtelijke stichting die vanwege haar nationale belang onder toezicht staat van NWO. NWO-I is de werkgever voor de medewerkers van de negen instituten en het bureau NWO-I.

verschilt tussen KNAW en NWO-I, zijn er twee versies van de vragenlijst gemaakt. Beide zijn opgenomen in bijlage 1.
Deze vragenlijst is vervolgens besproken met de vertegenwoordigers van de KNAW en NWO-I uit de klankbordgroep. In de klankbordgroep zitten inhoudsdeskundigen vanuit de koepelorganisaties en kennisinstellingen die vanuit hun kennis over de inhoud en het veld ons als onderzoeksteam en het ministerie van OCW als opdrachtgever adviseren over het onderzoek. De klankbordgroep bestond uit vertegenwoordigers van UNL, VH, NWO-I, KNAW, aangevuld met leden vanuit individuele universiteiten, hogescholen en UMC's.

Tabel 1.1 Onderzoeksopzet KNAW- en NWO-instituten in vogelvlucht

Fase	Activiteiten	Periode
Voorbereiding	• Aanpassen vragenlijst • Bespreking vragenlijst met klankbordgroep	Juni tot en met september 2023
Uitvoering zelfevaluatie door de instellingen	• Uitzetten vragenlijst en persoonlijk contact • Invullen vragenlijst door instituten • Nazorggesprek en duiding	Oktober en november 2023
Kwalitatieve verdieping	• Selectie en benadering cases • Uitvoering en verslaglegging cases	December 2023 Januari en februari 2024
Analyse en rapportage	• Analyse vragenlijsten • Rapportage • Bespreken conceptrapport met klankbordgroep	December 2023 tot maart 2024

1.3.2 Uitvoering zelfevaluatie

De goedgekeurde vragenlijst voor de zelfevaluatie voor het sectorbeeld onderzoeksinstituten KNAW en NWO-I is oktober 2023 uitgezet onder de centrale coördinatoren kennisveiligheid van KNAW en NWO-I via een beveiligde omgeving. Deze is bij NWO-I vervolgens door het bureau in samenspraak met de onderzoeksinstituten ingevuld. Bij de KNAW zijn de decentrale vragenlijsten ingevuld door de instituten zelf. Met de contactpersonen hielden we ook direct contact over de voortgang, eventuele vragen en tijdige oplevering.

In afstemming tussen de onderzoekers, het ministerie van OCW en de KNAW zijn de Fryske Akademy, het Rathenau Instituut en NIAS (Netherlands Institute for Advanced Study in the Humanities and Social Sciences) niet meegenomen in dit onderzoek vanwege hun andere institutionele positionering of omdat ze geen of nauwelijks onderzoek verrichten. Het Huygens Instituut, IISG en Meertens Instituut zijn gezamenlijk geconsulteerd omdat zij voor hun ondersteuning samenwerken in het Humanities Cluster. In paragraaf 2.2 geven we een beschrijving van de KNAW- en NWO-instituten. Uiteindelijk hebben 9 KNAW-instituten de zelfevaluatie ontvangen en ingevuld en hebben alle 9 NWO-instituten de zelfevaluatie ontvangen en ingevuld. Daarnaast hebben de KNAW- en NWO-I-bureaus allebei vragenlijsten ontvangen en ingevuld.

1.3.3 Aanvullend kwalitatief verdiepend onderzoek

Na de analyse van de vragenlijsten volgde een kwalitatief, verdiepend casestudy onderzoek bij de bureaus van de KNAW en NWO-I, bij twee onderzoeksinstituten van de KNAW en twee onderzoeksinstituten van NWO-I. Doel was om meer kwalitatieve informatie op te halen over het implementatieproces van de Leidraad, risicomanagement en risicoanalyses en over geleerde lessen,

aandachtspunten en dilemma's. De informatie uit deze onderzoeksfase vult het brede beeld uit de vragenlijst aan met meer diepgaand inzicht in beleidsprocessen en uitdagingen. Bij de selectie hebben we gezocht naar een spreiding over:

- achtergrondkenmerken (onderzoeksgebied, geografische spreiding en aantallen medewerkers); en
- inhoudelijk relevante praktijken op omgang met verschillende type risico's, op basis van de zelfevaluatie.

De criteria voor de selectie van cases en de leidraad voor de gesprekken zijn afgestemd en besproken met de opdrachtgever en de coördinatoren van de KNAW- en NWO-I-bureaus. Vanwege anonimiteit van de deelnemende instellingen, is de daadwerkelijke selectie gedaan door het onderzoeksteam in overleg met de coördinatoren van de KNAW- en NWO-I-bureaus en *niet* gecommuniceerd met de klankbordgroep of het ministerie van OCW. Voor elke case voerden we gesprekken met betrokkenen op meerdere niveaus binnen de instituten. Hierbij onderscheiden we het niveau van het bureau (waaronder de bestuurlijk portefeuillehouder en coördinator), en de onderzoeksinstituten (waaronder instituutsbestuurders en ondersteunende functies). In totaal zijn 13 personen gesproken.

1.3.4 Analyse en rapportage

Het onderzoeksteam heeft de door de instellingen aangeleverde informatie gecodeerd om vervolgens een inhoudelijke analyse op geaggregeerd niveau te maken. Daarbij hebben we waar mogelijk eenduidige vragen gekwantificeerd. De resultaten uit die analyse en de analyse van de caseverslagen zijn samengebracht in dit sectorbeeld voor de onderzoeksinstituten van KNAW en NWO-I.

2 Afbakening en ontwikkeling kennisveiligheidsbeleid

In dit hoofdstuk gaan we eerst in algemene zin in op het kennisveiligheidsbeleid van onderzoeksinstituten van KNAW en NWO-I. In paragraaf 2.1 beginnen we met de afbakening van het beleidsthema kennisveiligheid. In paragraaf 2.2 beschrijven we het proces van beleidsontwikkeling aan onderzoeksinstituten van KNAW en NWO-I.

2.1 Afbakening kennisveiligheid en diversiteit in de sector

De Nationale Leidraad Kennisveiligheid introduceert kennisveiligheid als volgt (pp. 8-9):

> Met kennisveiligheid wordt in deze leidraad in de eerste plaats bedoeld: het voorkomen van ongewenste overdracht van sensitieve kennis en technologie met negatieve gevolgen voor onze nationale veiligheid en de Nederlandse innovatiekracht.
> Daarnaast gaat het om heimelijke beïnvloedings- en inmengingsactiviteiten van statelijke actoren in hoger onderwijs en wetenschap. Dergelijke beïnvloeding (*foreign interference*) kan leiden tot vormen van (zelf)censuur resulterend in aantasting van de academische vrijheid.
> Tot slot draait het bij kennisveiligheid om ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd. Zo kunnen onderzoekers van uw instelling betrokken raken bij de ontwikkeling van technologie die in deze landen wordt ingezet bij de onderdrukking van de eigen burgers.

De Leidraad sluit hiermee aan op de afbakening van het ministerie van OCW zoals gegeven in de kamerbrief van november 2020.[13] In dit rapport schrijven we in het kort over **sensitieve kennis en technologie**, **heimelijke beïnvloeding** en **ethische kwesties** als de onderwerpen van kennisveiligheid.

De KNAW- en NWO-instituten kennen een grote diversiteit, met verschillen tussen de KNAW en NWO-I en variatie tussen de instituten onderling. NWO-I is een zelfstandige privaatrechtelijke stichting onder toezicht van NWO, waaronder negen onderzoeksinstituten zijn samengebracht.[14] NWO-I had in 2022 een budget van €221 miljoen. In 2022 kende NWO-I 1.598 fte (1.717 personen) aan medewerkers, waarvan 522 fte wetenschappelijk personeel (33%). Instituten verschillen in grootte van enkele tientallen medewerkers tot enkele honderden. Het centrale bureau NWO-I bestaat uit 50 personen.[15]

De KNAW kent twaalf instituten. Daarnaast zijn het Rathenau Instituut en de Fryske Akademy gelieerd aan de KNAW, maar zij hebben een zelfstandig bestuur. Het Huygens Instituut, Meertens Instituut en Internationaal Instituut voor Sociale Geschiedenis (IISG) hebben hun onderzoeksondersteuning gezamenlijk georganiseerd in het Humanities Cluster. DANS en NIAS (Netherlands Institute for Advanced Study in the Humanities and Social Sciences) bieden infrastructuur voor onderzoek en voeren in mindere mate zelfstandig onderzoek uit in vergelijking met de andere instituten. De KNAW-instituten hadden in 2019 een gezamenlijk budget van €128 miljoen. In 2019 was 1.166 fte werkzaam bij de instituten, waarvan 47% wetenschappelijk personeel.[16] Instituten verschillen in grootte van enkele tientallen medewerkers tot enkele honderden. Het KNAW stafbureau bestaat uit 130 personen.[17]

---

13 kamerbrief over maatregelen kennisveiligheid hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl
14 NWO-I - koepel voor onderzoekers | NWO
15 Kengetallen - NWO-I
16 Structuur van de Nederlandse kennisinfrastructuur | Rathenau Instituut
17 Stafbureau KNAW - KNAW

Bij zowel de KNAW als NWO-I wordt het kennisveiligheidsbeleid gecoördineerd vanuit de centrale bureaus. De coördinatoren bij beide bureaus zijn aanjagers voor de beleidsontwikkeling en risicoanalyses en ondersteunen instituten bij vragen omtrent kennisveiligheid. De beleidsontwikkeling en vaststelling ligt bij de bureaus en in de samenwerking, de implementatie en instituut-specifieke invulling ligt bij de instituten. Hierin verschillende de KNAW en NWO-I niet van elkaar. In de volgende hoofdstukken beschrijven we het kennisveiligheidsbeleid van de KNAW en NWO-I en hun instituten dan ook gezamenlijk; wanneer de KNAW en NWO-I verschillen in hun aanpak, benoemen we dit.

De definitie en afbakening van kennisveiligheid en beleid wordt door de beide bureaus gecoördineerd en geharmoniseerd. Zowel de KNAW als NWO-I vertrekken vanuit de definitie van kennisveiligheid van de Leidraad, met primair aandacht voor ongewenste overdracht van sensitieve kennis en technologie. Ook ligt de aandacht in sterkere mate op nationale veiligheid (onder meer *dual use*) en minder op innovatiekracht of economische veiligheid.

2.2 Ontwikkeling van kennisveiligheidsbeleid

De ontwikkeling van de Leidraad vormde voor zowel de KNAW als NWO-I aanleiding om te starten met implementatieprogramma's voor kennisveiligheidsbeleid. De KNAW is eind 2022 gestart met de beleidsvorming op kennisveiligheid, wat onder meer leidde tot een position paper in 2023.[18] De uitvoering van kennisveiligheidsbeleid begon in 2022 met de aanstelling van de coördinator. Eind 2023 is een implementatieplan vastgesteld dat sindsdien wordt uitgevoerd. Bij NWO-I is de beleidsvorming medio 2021 begonnen tijdens de voorbereiding op de Leidraad. Medio 2022 is een implementatieplan vastgesteld dat sindsdien wordt uitgevoerd en een coördinator aangesteld. Het bureau en de instituten hebben gezamenlijk een NWO-I-brede richtlijnen opgesteld, die per instituut wordt geïmplementeerd. Bij zowel de KNAW als NWO-I is begonnen met het inrichten van de verantwoordelijkheden en overlegstructuren en beschermingsmaatregelen.

De KNAW- en NWO-instituten hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel 2.1).[19] De risicoanalyses (het continu inschatten van risico's bij nieuwe samenwerkingen, werknemers, inkomende gasten, etc.) zijn bij zowel de KNAW als NWO-I volledig bij de instituten belegd met begeleiding van de bureaus. Op de overige onderdelen geldt voor NWO-I dat beleid deels nog in ontwikkeling is en deels is vastgesteld. Bij de KNAW is beleid veelal (deels) vastgesteld, met uitzondering van het personeelsbeleid dat nog in ontwikkeling is. Daarbij zien we een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad:

- Beleid op fysieke en digitale bescherming is vaker vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid.
- Beleid op het aangaan van (risicovolle) internationale partnerschappen is bij de KNAW en NWO-I op het niveau van de bureaus vastgesteld met aantoonbare uitvoering. Daarnaast is de implementatie van het beleid uitgevraagd bij de NWO-instituten, die in verschillende fases van beleidsimplementatie zitten.[20]

---

18 KNAW (2023). Kennisveiligheid - KNAW position paper, p. 2.

19 Deze rubric is afgeleid van de volwassenheidsniveaus zoals die worden gebruikt in bijvoorbeeld het SURFaudit toetsingskader IBHO, het toetsingskader MBO Digitaal en toetsingskader PO-VO Kennisnet. De rubric is eerder ook toegepast in de sectorbeelden universiteiten en hogescholen.

20 Dit is niet uitgevraagd bij de individuele KNAW-instituten.

- Beleid op toepassing van juridische kaders (voor compliance met export controle en sanctieregimes) ontbreekt relatief vaker dan de andere onderdelen van het kennisveiligheidsbeleid.
- De vertaling van kennisveiligheid in het personeelsbeleid is bij de meerderheid van de instituten vastgesteld met aantoonbare uitvoering.

Tabel 2.1. Zelfscores op fase van beleidsontwikkeling. (een aantal instituten heeft op één of meer onderdelen geen score ingevuld, hierdoor verschilt de n per onderwerp)

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en uitvoering aantoonbaar	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig
Risicoanalyse	1	6	6	3	2	
Risicomanagement	1	6	3	5	1	2
Fysieke en digitale beschermings-maatregelen	1	2	2	9	2	2
Internationale partnerschappen (NWO-instituten)	1	2	2	2		
Juridische kaders	7	1		5	1	
Personeelsbeleid	3	3	2	7		3

Evaluaties van het kennisveiligheidsbeleid worden nog niet structureel toegepast, omdat beleid nog in ontwikkeling is of nog niet lang genoeg wordt uitgevoerd. Zowel de KNAW als NWO-I verwachten in de tweede helft van 2024 voor de eerste maal hun kennisveiligheidsbeleid (formeel) te evalueren.

3 Risicoanalyses

De minister van OCW heeft op 4 april 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren.[21] Met een risicoanalyse identificeert een kennisinstelling welke risico's er zijn op kennisveiligheid. Volgens de Leidraad wordt hierbij gekeken naar drie samenhangende factoren:

(1) de inhoud van kennisgebieden,
(2) het land waar de betrokken samenwerkingspartner gevestigd is en
(3) de samenwerkingspartner zelf.

Door deze factoren integraal te bekijken, wordt een inschatting van de risico's gemaakt. Door de risico's van een instituut nauwkeurig in kaart te brengen, kan effectief beleid in worden gezet voor risicobeperking (bijvoorbeeld preventief beleid als het gaat om internationale partnerschappen of personeelsbeleid, en risicomanagement).

In dit hoofdstuk beschrijven we dit verzoek en de nieuwe of andere activiteiten die de instituten hebben ontplooid op basis van de oproep van de minister. Ook gaan we in op de manier waarop de instituten de risicoanalyses uitvoeren als onderdeel van het eigen kennisveiligheidsbeleid.

3.1 Risicoanalyse 2022

3.1.1 Verzoek van de minister

In de brief die de minister aan de kennisinstellingen stuurde, beschrijft hij de relevantie van kennisveiligheid en de daarvoor gezette stappen. Hierbij wijst hij op de publicatie van de Leidraad en de opening van het Rijksbrede Loket Kennisveiligheid.[22] De minister benadrukt het belang van het implementeren van de inhoud van de Leidraad binnen alle kennisinstellingen. Als onderdeel hiervan riep hij de kennisinstellingen op om op korte termijn (afronding kort na de zomer van 2022) een risicoanalyse rond kennisveiligheid uit te voeren of te actualiseren, om zo een scherp en volledig beeld te verkrijgen van de bijzonder waardevolle kennisdomeinen, risico’s en kwetsbaarheden binnen de instellingen.

Voor de praktische invulling van de risicoanalyse wordt verwezen naar de Leidraad en de mogelijkheid om contact op te nemen met het Loket Kennisveiligheid voor informatie en advies vanuit de Rijksoverheid. De minister erkent dat er grote verschillen bestaan tussen instellingen. Hij geeft daarom aan dat het doel van de risicoanalyse is dat vanuit de eigen instelling wordt bekeken wat het risicoprofiel is en of er verdere maatregelen nodig zijn om beter in control te zijn, zodat risico’s eerder worden gesignaleerd en er adequaat gehandeld wordt.

3.1.2 Invulling van de risicoanalyse door KNAW- en NWO-instituten

De coördinator kennisveiligheid en de CISO van het KNAW-bureau en het NWO-I-bureau hebben na de oproep van de minister de instituten getraind en ondersteund bij het uitvoeren van de risicoanalyse. Vrijwel alle instituten (16 van 18) geven dan ook aan naar aanleiding van de oproep van de minister een risicoanalyse te hebben uitgevoerd. Twee instituten geven aan dat ze geen eigen risicoanalyse hebben

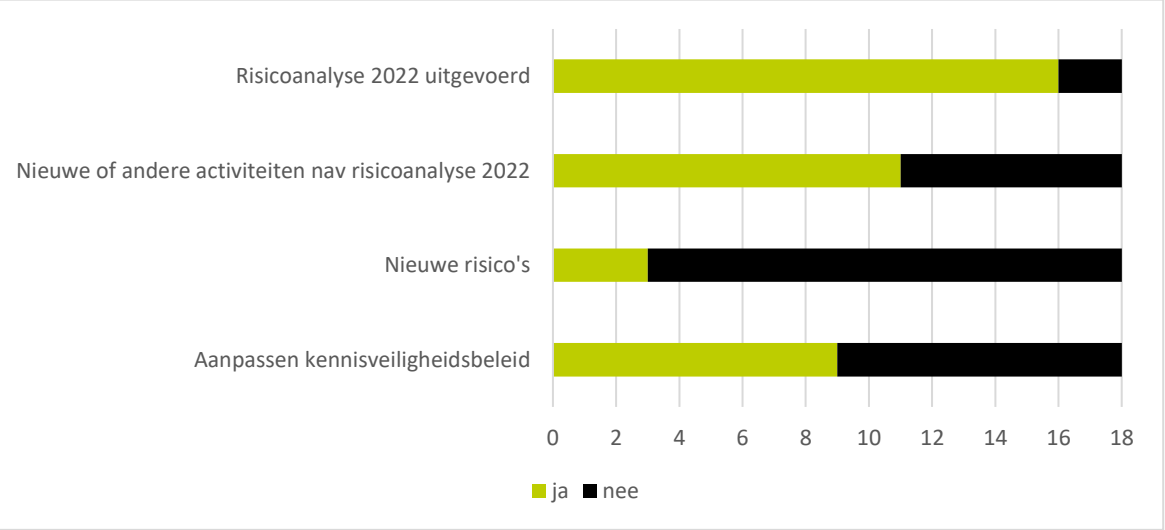
[21] Afschrift brief aan kennisinstellingen Nationale Leidraad Kennisveiligheid | Brief | Rijksoverheid.nl
[22] Zie Home | Loket Kennisveiligheid

uitgevoerd op instituutsniveau, omdat ze dit minder relevant achtten voor het type samenwerkingen of onderzoek dat wordt uitgevoerd. Eén van deze instituten geeft aan wel voor enkele projecten een risicoanalyse te hebben uitgevoerd.

De helft van de KNAW- en NWO-instituten (9 van de 18) geeft aan dat de oproep van de minister en de daaraan gekoppelde risicoanalyse hun eerste ervaring was met het uitvoeren van een risicoanalyse in het kader van kennisveiligheid. Drie instituten hebben op basis van de risicoanalyse nieuwe risico's geïdentificeerd. 11 instituten geven aan dat zij naar aanleiding van de oproep van de minister nieuwe of andere activiteiten hebben ontplooid in vergelijking met risicoanalyses die de instelling daarvoor uitvoerde. Vaak gaat dit over het geven van opvolging aan de geïdentificeerde risico's of het aanscherpen en verbreden van screeningsbeleid voor nieuwe medewerkers of samenwerkingen.

Er bestaan verschillende modellen aan de hand waarvan risicoanalyses kunnen worden uitgevoerd. Beide bureaus hebben gebruik gemaakt van het KWAS-model van de AIVD en hebben ondersteuning gegeven aan de risicoanalyses binnen de instituten. Het KNAW-bureau heeft ook contact gehad met de AIVD over het uitvoeren van de risicoanalyse. De meeste instituten (13 van de 18) geven aan gebruik te hebben gemaakt van het KWAS-model. Eén instituut heeft gebruik gemaakt van het model Risicoanalyse van UNL. Twee instituten geven aan gebruik te hebben gemaakt van de interim CISO die bekend was met het KWAS-model, en rapporteren hierbij niet over een gebruikt model. Voor twee andere instituten is het niet bekend of en welk model gebruikt is; zij geven dus niks aan over een gebruikt model.

Figuur 3.1 Overzicht activiteiten op risicoanalyses (n=18)



Over de resultaten van de uitgevoerde risico's geven de bureaus aan dat de risicoanalyses tot meer inzicht in en bewustwording van de risico's bij de verschillende instituten hebben geleid. Drie instituten hebben volgens hun beantwoording van de vragenlijst op basis van de risicoanalyse nieuwe risico's of kwetsbaarheden geïdentificeerd. Hierbij worden verschillende onderwerpen genoemd, zoals risico's op het gebied van sensitieve informatie, kroonjuwelen en personeelsbeleid. De instituten noemen dat dit vooral input biedt voor het aanscherpen van hun kennisveiligheidsbeleid.
Dat er bij veel instituten volgens de ingevulde vragenlijsten geen nieuwe risico's zijn geïdentificeerd, zegt niet dat de risicoanalyse geen effect heeft gehad: elf instituten rapporteren dat het uitvoeren van de risicoanalyse heeft geleid tot nieuwe (voorgenomen) maatregelen. Maatregelen richten zich bijvoorbeeld op het gebied van bewustwording, dienstreizen, samenwerking met instellingen uit landen

met een verhoogd risicoprofiel en personeelsbeleid. Ook geven enkele instituten aan dat het bewustzijn van kennisveiligheid verder verdiept is dankzij de risicoanalyse.

3.2 Risicoanalyse als onderdeel van het kennisveiligheidsbeleid

De meerderheid van instituten (12 van de 18) geeft aan dat hun beleid op het gebied van risicoanalyse in ontwikkeling is, of deels al is vastgelegd en uitvoering aantoonbaar. Eén instituut geeft aan geen beleid te hebben, de overige instituten geven aan dat het beleid volledig is vastgesteld en uitvoering aantoonbaar, of ook al een verbetercyclus kent. Eén instituut geeft aan dat het beleid zich eigenlijk geheel richt op informatiebeveiliging, wat in principe niet onder de afbakening van kennisveiligheid in dit onderzoek valt. Een ander instituut noemt dat het kennisveiligheidsbeleid in de breedte in ontwikkeling is, maar op informatiebeveiliging al is vastgesteld. In de verdiepende gesprekken is aangedragen dat instituten bij het ontwikkelen van het beleid voor risicoanalyses zoeken naar een goede balans tussen geformaliseerd beleid en het benutten van de kleinschaligheid van de instituten. Door de kleinschaligheid van de instituten, is er direct contact met onderzoekers mogelijk waardoor makkelijker in gesprekken gemonitord kan worden of er relevante casussen spelen. Dit lijkt voor sommige coördinatoren effectiever dan formele richtlijnen.

De risicoanalyses van de instituten bestaan uit verschillende onderdelen. In de Leidraad wordt hierbij onderscheid gemaakt tussen (a) het identificeren van sensitieve kennisgebieden, (b) het hanteren van een eigen lijst van sensitieve kennisgebieden, (c) het identificeren van ‘kroonjuwelen’ en (d) gestandaardiseerde processen die bij een bepaald risiconiveau in werking treden.

Tabel 3.1. Onderdelen risicoanalyses KNAW en NWO-I

	Uitgevoerd	(Nog) niet toegepast
Identificatie sensitieve kennisgebieden	13	5
Eigen lijst sensitieve kennisgebieden	1	17
Identificatie kroonjuwelen	11	7
Standaard-processen	4	14

Vanuit de bureaus is aan instituten gevraagd om sensitieve kennisgebieden of kroonjuwelen in kaart te brengen. Vrijwel alle instituten (16 van de 18) hebben dit gedaan als onderdeel van de risicoanalyse op verzoek van de minister (zie vorige paragraaf). Een aantal instituten geeft hierbij aan de definities en afbakening van begrippen als ‘sensitieve kennisgebieden’ en ‘kroonjuwelen’ niet helder of eenduidig gedefinieerd zijn (zie ook paragraaf 3.3). Op dit moment interpreteren de instituten de term ‘kroonjuwelen’ op verschillende manieren. Sommige instituten richten zich vooral op (mogelijke) dual-use technologieën. Andere instituten bestempelen bijvoorbeeld het imago van het instituut als kroonjuweel, omdat de naam van het instituut op het cv van een onderzoeker toegang kan geven tot andere organisaties of kennisinstellingen. De meeste instituten kiezen er niet voor om een eigen lijst van sensitieve kennisgebieden te hanteren.

De KNAW en NWO-I hanteren richtlijnen voor standaardprocessen die in werking treden bij bepaalde risiconiveaus, bijvoorbeeld bij het aangaan van internationale partnerschappen. Bij de beleidsimplementatie op instituutsniveau kiezen instituten er vaak voor om het beleid op meer informele wijze uit te voeren. Aangegeven wordt dat door de kleinschaligheid van instituten en de

beperkte schaal waarop zij te maken hebben met kennisveiligheidsrisico's een informele werkwijze de voorkeur geniet. Ook geven de meeste instituten aan (nog) niet op structurele wijze en continu de risico's ten aanzien van kennisgebieden en kroonjuwelen bij te houden.

3.3 Dilemma's en aandachtpunten

Vanuit de instituten hebben we een drietal algemene dilemma's en aandachtspunten gedestilleerd:

- Kennisveiligheid is niet voor alle instituten op dezelfde manier en in dezelfde mate relevant. Zo wordt er aangegeven dat het kennisveiligheidsbeleid vaak ver afstaat van sociale en geesteswetenschappen. Ook worden bij uiterst fundamenteel onderzoek minder risico's gezien. Het is moeilijk om eventuele toekomstige kennisveiligheidsrisico's bij nog onbekende toepassingen vast te stellen. Ook geven sommige instituten aan dat zij zich vooral richten op informatieveiligheid, maar dat andere aspecten die worden gekoppeld aan kennisveiligheid voor hen niet relevant zijn. Daarom ervaren sommige instituten het als minder relevant en proportioneel om een risicoanalyse op gestructureerde wijze en op alle gevraagde onderdelen uit te voeren.
- Een aantal instituten geeft aan dat Open Science een van de belangrijkste waarden binnen het instituut is, en dat dit als strijdig wordt ervaren met het voeren van beleid op het gebied van kennisveiligheid. Zij willen bijvoorbeeld in het delen van hun resultaten geen onderscheid maken tussen landen.
- Verschillende instituten geven in de vragenlijst en de casestudies aan behoefte te hebben aan een concretisering van definities op nationaal niveau. Zij vragen zich met name af wat er precies bedoeld wordt met kroonjuwelen, en geven aan dat overzichten van sensitieve kennisgebieden vaak niet bruikbaar zijn voor specifieke onderzoeksvelden of -thema's. Sommige respondenten vragen zich af of het überhaupt mogelijk is om een lijst van sensitieve kennisgebieden op te stellen die in de breedte van het hele onderzoeksveld te gebruiken is.

3.4 Lessons learned

Uit de analyse van de instituten worden twee lessons learned gedestilleerd. De instituten zijn over het algemeen kleinschalig ingericht. Hierdoor zijn de 'lijntjes' binnen de instituten vaak korter. Meerdere keren is genoemd dat het vanwege deze korte lijntjes niet noodzakelijk is om regelmatig formele risicoanalyses uit te voeren, maar dat betrokkenen op het gebied van kennisveiligheid elkaar onderling weten te vinden en monitoren of er nieuwe risicovolle casussen optreden. Het persoonlijke contact helpt volgens de instituten om vervolgens op een goede manier met deze casussen om te gaan.

De bureaus hebben een aanpak voor de risicoanalyse vormgegeven en de instituten hier actief bij ondersteund. Dit hielp om de risicoanalyse uit te voeren binnen de instituten omdat deze toegespitst werd op de context van de instituten en omdat er makkelijk contact kon worden gezocht met ondersteuning vanuit het centrale bureau.

4 Risicomanagement en fysieke en digitale maatregelen

In dit hoofdstuk beschrijven we hoe de KNAW en NWO-I risicomanagement hebben belegd en vastgelegd. Het gaat hier om de (al dan niet geformaliseerde) verdeling van verantwoordelijkheden en processen om kennisveiligheidsvraagstukken binnen de organisatie te behandelen. Ook gaan we in op het toegangsbeleid tot ruimtes en digitale gegevens als onderdeel van risicomanagement. Tot slot bespreken we de dilemma's en uitdagingen specifiek op dit onderdeel van het kennisveiligheidsbeleid, gevolgd door *lessons learned*.

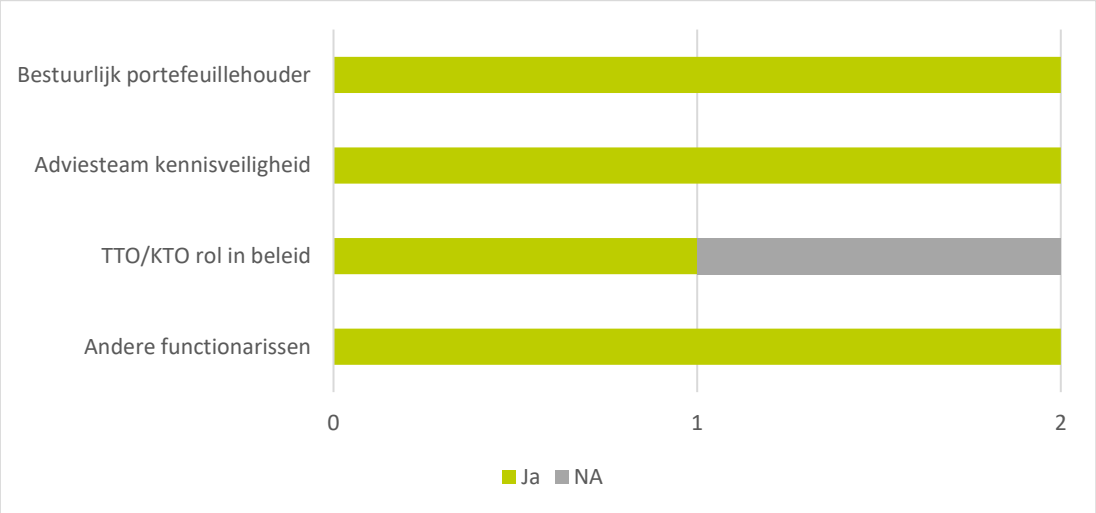
4.1 Organisatie risicomanagement

In deze paragraaf beschrijven we hoe kennisveiligheid organisatorisch is vormgegeven en hoe verantwoordelijkheden zijn belegd. Hierbij volgen we de aanbevelingen van de Leidraad.

Het beleid voor risicomanagement van kennisveiligheid krijgt bij zowel het KNAW-bureau als het NWO-I-bureau de aandacht. Het KNAW-bureau geeft aan dat het beleid is vastgesteld en de uitvoering aantoonbaar is. Het NWO-I-bureau geeft aan dat delen van het beleid in verschillende fases zitten. Het beleid is deels in ontwikkeling, deels vastgesteld met een uitvoering die aantoonbaar is en voor een deel van het beleid is al een verbetercyclus aanwezig. De meeste instituten hebben aandacht voor beleid rondom risicomanagement van kennisveiligheid (zie eerder Tabel 2.1). Acht instituten geven aan beleid omtrent risicomanagement van kennisveiligheid te hebben wat (deels) is vastgesteld en waarvan de uitvoering aantoonbaar is. Drie instituten geven aan dat er voor dit beleid al (deels) een verbetercyclus aanwezig is. Zes instituten geven aan dat dit beleid nu in ontwikkeling is, slechts één instituut geeft aan geen beleid te hebben.

Figuur 4.1 en 4.2 geven een meer specifiek overzicht van de activiteiten van de KNAW en NWO-I op het gebied van risicomanagement op – eerst – centraal niveau, en daarna op instituutsniveau.

Figuur 4.1 Overzicht activiteiten risicomanagement op niveau van bureaus (n=2)



De KNAW- en NWO-I-bureaus hebben op centraal niveau een **bestuurlijk portefeuillehouder** kennisveiligheid aangewezen. Bij het KNAW-bureau valt deze portefeuille onder de taken van de president, bij het NWO-I-bureau is een van de instituutsdirecteuren verantwoordelijk.
In de verdiepende gesprekken bij de KNAW geven respondenten aan dat de bestuurlijk portefeuillehouder kennisveiligheid zich in de breedte met het onderwerp bezig houdt en deelneemt aan de landelijke regiegroep kennisveiligheid. De KNAW-directie is eindverantwoordelijk voor de instituten en is vanuit die rol ook verantwoordelijk voor de besluitvorming voor beleid omtrent kennisveiligheid. De bestuurlijk portefeuillehouder wordt ondersteund door de coördinator kennisveiligheid.
In de verdiepende gesprekken geeft NWO-I aan dat de bestuurlijk portefeuillehouder kennisveiligheid ad hoc betrokken wordt bij casussen en op de hoogte blijft van landelijk en internationaal beleid en ideeën omtrent kennisveiligheid. De bestuurlijk portefeuillehouder wordt ondersteund in de rol door o.a. de coördinator kennisveiligheid van het NWO-I-bureau.

4.1.1 Organisatieonderdelen betrokken bij kennisveiligheid

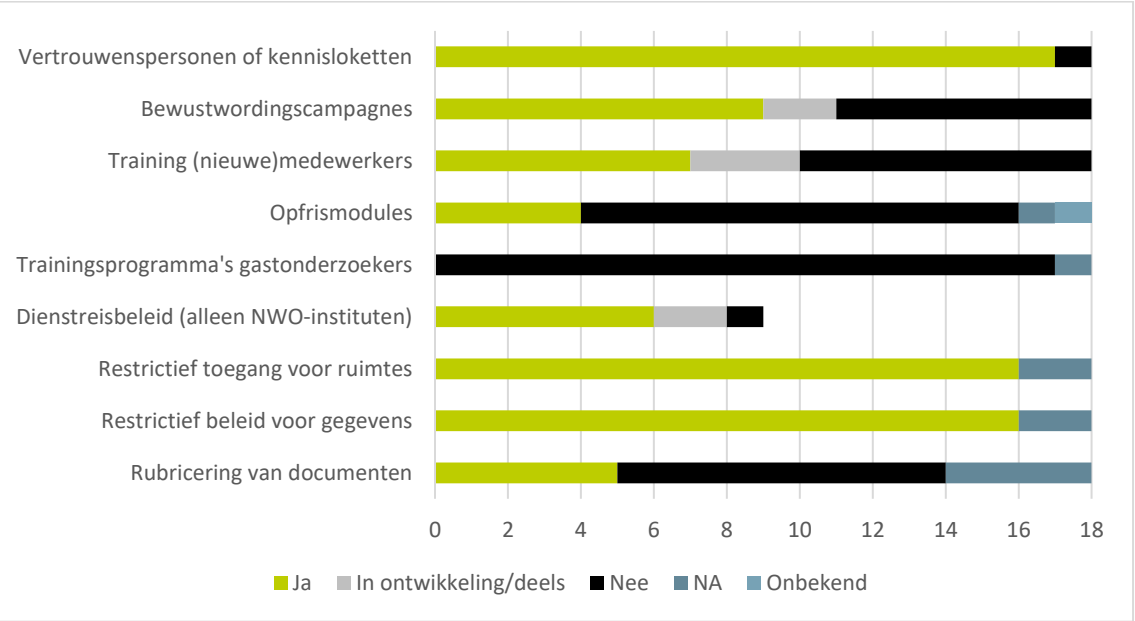
Zowel het KNAW- als NWO-I-bureau hebben een **adviesteam Kennisveiligheid** ingesteld. Het KNAW-bureau geeft aan een adviesteam te hebben ingericht met de coördinator kennisveiligheid, een jurist en een medewerker van het KTO. Daarnaast geeft het KNAW-bureau aan dat ze indien nodig medewerkers met aanvullende kennis betrekken. Naast het adviesteam heeft de KNAW een werkgroep waarin elk instituut is vertegenwoordigd. Deze contactpersonen kennisveiligheid komen uit verschillende lagen en operationele functies binnen de instituten, bijvoorbeeld groepsleiders, hoofden ICT of hoofden datamanagement.
Het NWO-I-bureau geeft aan dat het adviesteam voortbouwt op een eerder opgezette werkgroep kennisveiligheid. Het adviesteam heeft leden uit elk instituut en vertegenwoordiging van alle lagen en operationele functies (o.a. HR, ICT, management). Het adviesteam helpt met het inbedden van kennisveiligheidskwesties in bestaande overlegstructuren door de betrokkenheid van medewerkers met verschillende functies. Daarnaast bevordert de aanwezigheid van elk instituut in het adviesteam de samenhang in ontwikkelingen en afwegingen over kennisveiligheid tussen de NWO-instituten. De leden van het adviesteam fungeren binnen het eigen instituut als contactpersoon kennisveiligheid om een laagdrempelig aanspreekpunt te hebben voor medewerkers bij alle instituten. Het verkrijgen van beleidsmatige afstemming tussen kennisveiligheidsbeleid en breder beleid van de instituten is bij beide organisaties belegd in bestaande overleggen zoals het directeurenoverleg, het instituutsmanagersoverleg en het bedrijfsvoeringsoverleg.

Uit de verdiepende gesprekken komt naar voren dat de werkgroep van de KNAW en het adviesteam van de NWO-I ook worden gebruikt voor kennisdeling. Vertegenwoordigers kunnen sparren over ideeën en dilemma's. De insteek is dat door gezamenlijk casuïstiek te bespreken de leden meer ervaring opdoen met kennisveiligheidskwesties en instituten elkaar kunnen ondersteunen in het ontwikkelen van werkwijzen hoe hier mee om te gaan. Gesprekspartners benoemen dat het regulier samenkomen in de werkgroep de leden ook helpt om op de hoogte te blijven van de politieke ontwikkelingen in het kennisveiligheidsdomein.

Leden van de adviesteams vinden het in verband met vertrouwelijkheid soms lastig om een afweging te maken tussen gedetailleerde dilemma's delen met de andere leden of casuïstiek toch algemener houden en niet verder verspreiden buiten het eigen instituut. Een andere respondent benoemt dat meer samenwerking gefaciliteerd kan worden binnen de werkgroep door nadruk te leggen op risico's die sommige instituten gemeen hebben.

Het KNAW-bureau geeft aan dat op centraal niveau **vertrouwenspersonen** aanwezig zijn waar medewerkers terecht kunnen, deze personen moeten nog wel gebriefd worden op het gebied van kennisveiligheid. Het NWO-I-bureau geeft aan dit voor nu op instituutsniveau belegd te hebben en is nog aan het onderzoeken of het gewenst is dit centraal in te regelen.
Het KNAW-bureau geeft aan dat op centraal niveau de **knowledge transfer office (KTO)** lid is van het adviesteam en vanuit daar betrokken is bij casuïstiek en zelf ook casuïstiek inbrengt. Het NWO-I-bureau heeft dit niet centraal belegd maar het verschilt per instituut hoe de betrokkenheid is geregeld, bijvoorbeeld door de valorisatiemanager te betrekken. NWO-I geeft aan dat kennisveiligheid zal worden meegenomen in de verdere ontwikkeling van het (centrale) kennisbenuttingsbeleid.

Figuur 4.2 Overzicht activiteiten risicomanagement op instituutsniveau (n=18)



Op bijna alle instituten (17 van de 18) zijn vertrouwenspersonen aanwezig waar medewerkers terecht kunnen met vragen en zorgen over kennisveiligheid. Deze vertrouwensfunctie is over het algemeen niet exclusief voor het melden van (kennis)veiligheidsrisico's, maar ook voor vragen over wetenschappelijke integriteit, databeveiliging, privacy vraagstukken en ongewenst gedrag. Dit betekent dat het instituut dat deze vraag met 'nee' heeft beantwoord niet noodzakelijkerwijs helemaal geen vertrouwenspersonen heeft, maar waarschijnlijk dat hun vertrouwenspersonen niet specifiek te benaderen zijn voor kennisveiligheidsvraagstukken. Zes instituten geven daarnaast aan dat voor specifieke vragen en zorgen medewerkers ook bij hun leidinggevende, coördinator kennisveiligheid, data/ICT managers of instituutsmanagers/directeuren terecht kunnen. Twee instituten geven aan dat is afgesproken dat de vertrouwenspersoon vragen en zorgen doorverwijst naar de coördinator kennisveiligheid, data/ICT managers of het management omdat de vertrouwenspersonen nog niet de expertise hebben om met kennisveiligheidskwesties om te gaan.

Ethische commissies, die onderzoeksvoorstellen beoordelen op ethische maatstaven, worden maar beperkt meegenomen in het kennisveiligheidsbeleid door de KNAW- en NWO-I-bureaus en de KNAW instituten. Hoewel ethische commissies een belangrijk organisatieonderdeel kunnen vormen voor het voorkomen van ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd (het derde onderdeel van de definitie van

kennisveiligheid), geven meerdere KNAW instituten aan dat dit niet van toepassing is op hun activiteiten. Een aantal instituten geeft aan gebruik te maken van de ethische commissie van het KNAW-bureau die ondersteuning en advies kan bieden. Er zijn ook ethische commissies die onafhankelijk van het kennisveiligheidsbeleid zijn georganiseerd, bijvoorbeeld rondom ethische gedragscodes voor het uitvoeren van onderzoek met levende dieren. Het NWO-I-bureau heeft op centraal niveau geen ethische commissie. Ethische commissies worden niet genoemd als betrokken in adviesteams voor kennisveiligheid door de KNAW- en NWO-I-bureaus.

4.1.2 Ontwikkelen van bewustzijn van kennisveiligheid

Een essentieel onderdeel van het kennisveiligheidsbeleid is de inbreng van onderzoekers. Onderzoekers zijn, als inhoudelijk experts, noodzakelijk voor het signaleren van kennisveiligheidsrisico's en dienen daarom meegenomen te worden in het risicomanagement. De AWTI geeft in haar rapport 'Kennis in conflict' eveneens dit aandachtspunt (Aanbeveling 3. Realiseer: vergroot het bewustzijn en de capaciteit).

De helft van de instituten (9 van de 18) geeft aan **bewustwordingscampagnes** te voeren rondom kennisveiligheid. De KNAW en NWO-I hebben hiervoor beiden een vergelijkbare campagne laten ontwikkelen. Bij de KNAW staat de campagne voor 2024 op de planning. Bij NWO-I is de campagne al breed uitgerold en geven 8 van de 9 instituten aan deze toe te passen. Deze bewustwordingscampagnes zijn gericht op alle onderzoekers in alle lagen van de instituten. Daarnaast krijg kennisveiligheid in de managementoverleggen met groepsleiders en senior personeel aandacht, met het idee dat deze bewustwording doorstroomt naar de andere medewerkers van de teams.

Een deel van de instituten (7 van de 18) biedt informatie of trainingen gericht op **nieuwe medewerkers** voor de ontwikkeling van kennisveiligheidsbewustzijn. Meermaals is het onderwerp kennisveiligheid ingebed in bestaande trainingen over bijvoorbeeld informatie- en cyberveiligheid en privacy. Eén instituut noemt dat medewerkers rondom een kroonjuweel extra informatie krijgen voor (kennis)veiligheidsbewustzijn. Een deel van de instituten (8 van de 18) geeft aan geen informatie of trainingen voor nieuwe medewerkers te hebben, drie van de 18 zijn dit momenteel aan het ontwikkelen.

Het merendeel van de instituten (12 van de 18) biedt (nog) geen opfrismodules voor **zittend personeel**. Een aantal instituten geeft aan dat de bewustwordingscampagne nog in de uitrolfase zit, pas daarna komt de vraag hoe dit verder ingebed kan worden. Van de vier instituten die aangeven dat deze modules wel aanwezig zijn, maken drie gebruik van de modules binnen de bovengenoemde NWO-I brede bewustwordingscampagne en geeft één instituut aan dit zelf te hebben ingeregeld. Eén instituut geeft aan dat dit niet van toepassing is en voor één instituut is onbekend of deze opfrismodules aanwezig zijn.
Geen enkel instituut biedt speciale trainingsprogramma's gericht op academische kernwaarden specifiek voor **gastdocenten, gaststudenten of gastonderzoekers** uit landen met een verhoogd risicoprofiel. Een aantal instituten licht toe dat ze wel onboardings- en trainingsprogramma's hebben over academische/wetenschappelijke kernwaarden en data management, maar dat deze gericht zijn op alle wetenschappers.

4.1.3 Dienstreizen naar het buitenland

De KNAW en NWO-I-bureaus hebben centraal beleid heeft opgesteld over de omgang met **dienstreizen naar landen met een verhoogd risicoprofiel**. Bij de NWO-instituten geven acht van de negen instituten

aan dat ze een NWO-I-brede richtlijn geïmplementeerd hebben of nog aan het implementeren zijn.[23] Daarnaast noemt een vijftal instituten dat ze additionele regels hebben over het meenemen van IT-apparatuur naar het buitenland. Hierbij wordt genoemd dat soms lege of opgeschoonde laptops worden gebruikt of software wordt geïnstalleerd die toelaat op afstand het apparaat te wissen. Eén instituut geeft aan geen beleid te hebben maar dat er op casus niveau wordt gekeken door de leidinggevende en management.

In de verdiepende gesprekken komt naar voren dat het omgaan met privéreizen van medewerkers naar landen met een verhoogd risicoprofiel nog lastig wordt gevonden. De instituten hebben geen formele zeggenschap over de privéactiviteiten van hun medewerkers. Gesprekspartners geven aan hierover open te communiceren met de medewerkers om zo de drempel laag te houden voor vragen en advies en samen tot een pragmatische oplossing te komen.

4.2 Fysieke en digitale beschermingsmaatregelen

Een praktisch punt van aandacht binnen risicomanagement is de toegang tot fysieke en digitale omgevingen van de KNAW en NWO-I. De aandacht gaat hier uit naar het voorkomen dat personen ongewenst toegang krijgen tot ruimtes of gegevens. In deze paragraaf bespreken we hoe opvolging is gegeven aan de diverse aanbevelingen van de Leidraad.

De KNAW- als NWO-I-bureaus hebben beleid voor fysieke en digitale beschermingsmaatregelen op het vlak van kennisveiligheid. Het KNAW-bureau geeft aan dat het beleid is vastgesteld met aantoonbare uitvoering. Het NWO-I-bureau geeft aan dat delen van het beleid in verschillende fases zitten. Het beleid is zowel deels in ontwikkeling als deels vastgesteld (met een uitvoering die aantoonbaar is) en voor een deel van het beleid is al een verbetercyclus aanwezig.

Beleid voor fysieke en digitale beschermingsmaatregelen op het vlak van kennisveiligheid is op de meeste instituten aanwezig (zie eerder Tabel 2.1). Elf instituten geven aan beleid omtrent risicomanagement van kennisveiligheid te hebben wat (deels) is vastgesteld en waarvan de uitvoering aantoonbaar is. Vier instituten geven aan dat er voor dit beleid al (deels) een verbetercyclus aanwezig is. Twee instituten geven aan dat dit beleid nu in ontwikkeling is, slechts één instituut geeft aan geen beleid te hebben.

4.2.1 Restrictief toegangsbeleid voor ruimtes

Het merendeel van de instituten (16 van de 18) heeft een **restrictief toegangsbeleid voor bepaalde ruimtes** (zoals laboratoria of serverruimtes). De invulling hiervan verloopt veelal via elektronische toegangspassen die toegang verlenen tot ruimtes die van toepassing zijn op de activiteiten van de medewerker. Het beheer van de toegang gebeurt door verschillende medewerkers, bijvoorbeeld groepsleiders, leidinggevenden, management, veiligheidscoördinatoren of de receptie. Hierbij wordt meermaals genoemd dat dit niet alleen uit kennisveiligheidsoverwegingen is, maar bijvoorbeeld ook omtrent arbo-veiligheid, informatiebeveiliging en privacy. Twee instituten geven aan dat restrictief toegangsbeleid niet relevant is, bijvoorbeeld omdat het instituut geen ruimtes heeft waar dit nodig is.

[23] Dit is niet uitgevraagd bij de individuele KNAW-instituten.

Een groot deel van de instituten geeft aan dat **toegang van buitenlandse reisdelegaties** tot restrictieve ruimtes zeer zelden voorkomt. Als bezoek aan een restrictieve ruimte relevant is voor de reisdelegatie gebeurt dit altijd onder begeleiding van een medewerker. Eventueel wordt van te voren advies gevraagd van de coördinator kennisveiligheid of de directie hoe om te gaan met specifiek bezoek. Een aantal instituten geeft aan dat buitenlandse reisdelegaties geen toegang krijgen tot restrictieve ruimtes.

4.2.2 Restrictief toegangsbeleid voor onderzoeksgegevens en documenten

Het merendeel van de instituten (16 van de 18) geeft aan dat ze beleid hebben omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten. Meermaals wordt aangegeven dat dit beleid zich meer richt op omgang met gevoelige persoonsgegevens en informatieveiligheid (o.a. omtrent patenten) dan op kennisveiligheidsrisico's. Het grootste deel van de instituten met beleid geeft aan dat dit vaak op onderzoeksgroep of afdelingsniveau is gecompartimenteerd. Toegang wordt dan bepaald door de groepsleider of het afdelingshoofd en onderhouden door de ICT-afdeling. Eén instituut geeft aan dat er per dataset een keuze wordt gemaakt over welke personen toegang krijgen. Een ander instituut geeft aan dat alle data tussen medewerkers uitgewisseld mag in het kader van *open science*. Als er redenen zijn voor beperking van toegang wordt de data gecompartimenteerd en technisch afgeschermd. Twee instituten geven aan dat dit niet relevant is voor het eigen instituut.

Vijf van de 18 instituten geven aan beleid te hebben voor het rubriceren van documenten, denk aan labels als 'vertrouwelijk' of 'geheim'. De kwalificatie voor de rubricering zit meer in het beschermen van persoonsgegevens en andere vertrouwelijke data die wordt gebruikt in onderzoek. Het merendeel van de instituten (13 van de 18) geeft aan dat ze niet werken met rubricering of dat dit niet van toepassing is op de data die het instituut gebruikt. Hierbij noemen een aantal instituten dat data aangemerkt kan worden als privacygevoelig, maar dat dit niet met kennisveiligheid te maken heeft. Een aantal van deze instituten geeft aan nog na te denken of het rubriceren van documenten in de toekomst gewenst is.

De KNAW- en NWO-I-bureaus geven aan dat wordt overlegd en/of afgestemd met medewerkers betrokkenen bij het **cyberveiligheidsbeleid**. Het KNAW-bureau geeft aan dat dit structureel gebeurt door de deelname van de coördinator kennisveiligheid aan het reguliere overleg informatieveiligheid. Het NWO-I-bureau geeft aan dat in bewustwordingscampagnes zowel de onderwerpen rondom cyberveiligheid als kennisveiligheid zijn meegenomen en dat er overleg plaatsvindt tussen de betrokken medewerkers van beide domeinen.

Cyberveiligheid hangt samen met het kennisveiligheidsbeleid, maar kent een eigen beleidshistorie en wordt niet ontwikkeld met specifieke aandacht voor landen met een verhoogd risicoprofiel of sensitieve kennis. SURF brengt jaarlijks in beeld wat het cyberdreigingsbeeld[24] is in het hoger onderwijs en voert ook audits[25] uit van het cyberveiligheidsbeleid. In dit sectorbeeld laten we cyberveiligheid daarom verder buiten beschouwing.[26]

---

[24] SURF (2023). Cyberdreigingsbeeld 2023. Onderwijs en onderzoek.

[25] SURFaudit: inzicht en overzicht in je informatiebeveiliging en privacy | SURF.nl

[26] Net als het cyberveiligheidsbeleid vind het beleid rondom ethische toetsing van onderzoek reeds plaats buiten het kennisveiligheidsbeleid van instellingen. Een belangrijk verschil is echter dat het voor cyberveiligheidsbeleid niet uitmaakt waar dreiging vandaan komt; een hack is onwenselijk ongeacht het land van herkomst. Voor ethische toetsing is het echter wel van belang waar kennis of technologie wordt toegepast. Om deze reden zijn de beleidsmaatregelen rondom ethische risico's wel meegenomen in dit sectorbeeld.

4.3 Dilemma's en aandachtspunten

We observeren in dit onderzoek een aantal dilemma's en aandachtspunten gebaseerd op de zelf-evaluaties en verdiepende gesprekken: proportionaliteit, leveranciersselectie van onderzoeksinstrumentaria en privé reizen van medewerkers.

Een aantal instituten benoemt proportionaliteit als dilemma. Proportionaliteit is hier gerelateerd aan twee overwegingen: (1) de hoogte van het ingeschatte risicoprofiel en (2) de administratieve druk in het uitvoeren van kennisveiligheidsbeleid. Meerdere instituten geven aan dat ze inschatten een laag risicoprofiel te hebben. Vaak wordt hierbij genoemd dat ze onderzoek doen op een laag TLR-niveau (0-1) waardoor het vaststellen van eventuele kennisveiligheidsrisico's moeilijk is, want de mogelijke toepassingen zijn nog te breed.

Daarnaast ziet een aantal instituten de administratieve druk als een dilemma. Kennisveiligheidsbeleid, vastgelegde processen en protocollen kunnen helderheid scheppen voor het signaleren en mitigeren van kennisveiligheidsrisico's. Instituten geven echter tegelijkertijd aan dat het beleid niet moet leiden tot een bureaucratie die niet in relatie staat tot de (potentiële) risico's. Ook geldt hierbij dat de lijntjes binnen instituten vaak kort zijn, door de beperkte omvang van instituten, waardoor persoonlijk contact de voorkeur geniet boven meer bureaucratie (zie eerder paragraaf 3.4).

Een aantal instituten geeft aan dat ze het nog lastig vinden om kennisveiligheid mee te nemen in de leveranciersselectie van onderzoeksinstrumentaria of software. De afwegingen worden snel complex, waardoor het minder transparant wordt waarom de ene leverancier wordt vermeden en de andere niet. Daarbij willen instituten graag de kwalitatief beste instrumentaria gebruiken voor een onderzoek.

Een ander dilemma dat naar voren komt is hoe om te gaan met privéreizen naar hoog risicolanden. Als werkgever heeft een instituut hier geen invloed op, maar het kan wel kennisveiligheidsrisico's opleveren voor een instituut.

4.4 Lessons learned

De KNAW- en NWO-I-bureaus hebben beiden een werkgroep of adviesteam ingericht met vertegenwoordiging vanuit alle instituten en van verschillende werkdomeinen (ICT, HR, management etc.) en de coördinator kennisveiligheid van het centrale bureau. Deze opzet faciliteert samenwerking tussen de instituten en zorgt ervoor dat niet elk instituut voor zichzelf ervaring op hoeft te doen en beleid te ontwikkelen. De vertegenwoordiging van verschillende werkdomeinen zorgt ervoor dat kennisveiligheid vanuit verschillende perspectieven wordt bekeken en het beleid ontwikkeld wordt vanuit meerdere expertises en aan de hand van concrete casuïstiek.

In de zelfevaluaties en verdiepende gesprekken komt meermaals naar voren dat het creëren van awareness en draagvlak voor het kennisveiligheidsbeleid belangrijk is. De KNAW en NWO-I proberen awareness en draagvlak op twee manieren te vergroten. Ten eerste door beleid binnen de logica van huidige processen op de werkvloer in te brengen. Dit uit zich onder andere in het onderbrengen van kennisveiligheid in overkoepelende beleid op informatieveiligheid, bijv. in combinatie met cyberveiligheid; en door medewerkers uit verschillende werkdomeinen te betrekken in adviesteam en werkgroep. Ten tweede door duidelijk te communiceren over kennisveiligheidsbeleid en de

medewerkers mee te nemen in de redenering achter het beleid. In de verdiepende gesprekken werd meermaals benadrukt dat door de beperkte omvang van de instituten korte lijntjes mogelijk zijn en de coördinator kennisveiligheid van het bureau laagdrempelig toegankelijk is.

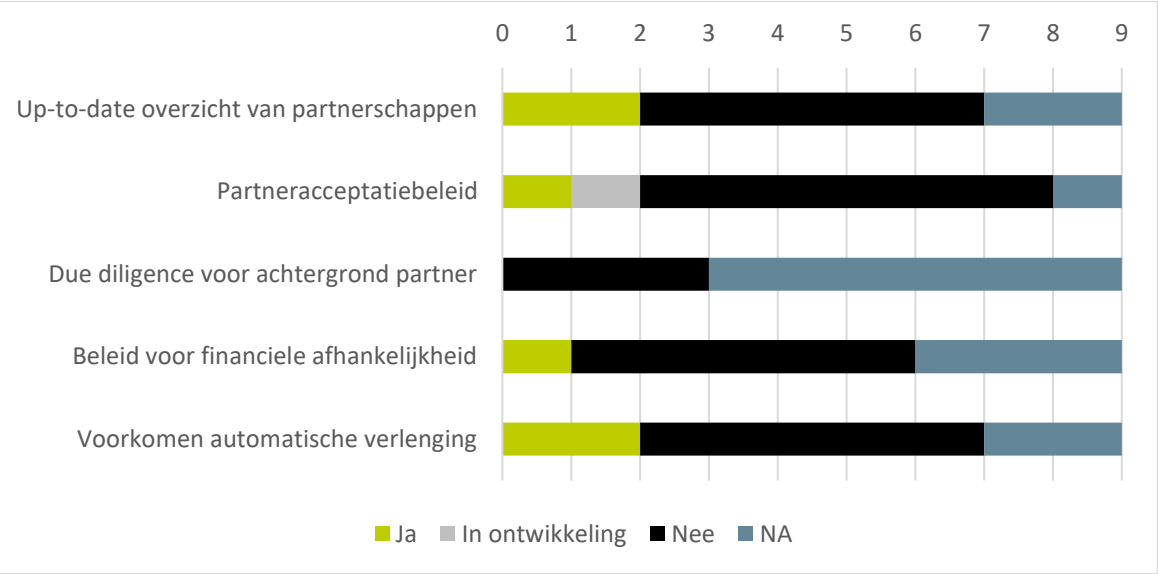
5 Internationale partnerschappen en juridische kaders

In dit hoofdstuk analyseren we het kennisveiligheidsbeleid omtrent internationale samenwerking. Hieronder verstaan we concrete partnerschappen en samenwerkingsverbanden die de KNAW, NWO-I en hun instituten aangaan met internationale organisaties en individuen, waarbij inhoudelijke of financiële toezeggingen worden gedaan en overeenkomsten worden afgesloten. Daarnaast bespreken we in dit hoofdstuk ook de juridische kaders voor internationale partnerschappen, zoals exportregels en sanctieregimes. We bespreken eerste de stand van zaken rondom deze thema's, en sluiten af met een overzicht van dilemma's, aandachtspunten en *lessons learned.*

5.1 Internationale partnerschappen

De KNAW en NWO-I hebben beleid ontwikkeld en in uitvoering op het aangaan van internationale partnerschappen, dat op instituutsniveau wordt geïmplementeerd. Bij de KNAW en NWO-I geldt dat partnerschappen met een hoog risico niet (meer) door instituten zelf kunnen worden aangegaan, maar dat deze dienen te worden geaccordeerd op centraal niveau door respectievelijk de KNAW-directie en de NWO-I-portefeuillehouder. Onder NWO-instituten is de fase van beleidsimplementatie ook per instituut uitgevraagd,[27] dit is weergegeven in Figuur 5.1.

Figuur 5.1 Overzicht activiteiten internationale partnerschappen van NWO-instituten (n=9)



5.1.1 Centraal overzicht partnerschappen en financiering

Om kennisveiligheidsbeleid te voeren op internationale partnerschappen, is het van belang dat er zicht is op de internationale partnerschappen. Het KNAW-bureau ontwikkelt een centraal overzicht van risicovolle partnerschappen voor alle instituten, op basis van het al bestaande overzicht van financiering en financieringsbronnen. Medio 2024 start KNAW met een uitvraag onder instituten naar hun veiligheidsgevoelige partnerschappen, dat wordt daarna centraal bijgehouden. Twee NWO-instituten hebben een overzicht van veiligheidsgevoelige partnerschappen. Bij de overige zeven NWO-instituten

[27] KNAW heeft dit centraal beantwoord omdat het beleid hetzelfde is voor alle instituten.

en het centrale NWO-I-bureau is zo'n overzicht nog niet aanwezig. NWO-I heeft in 2022 een quick-scan gedaan van partnerschappen, de ontwikkeling van een centraal overzicht staat gepland in 2024.
Het verkrijgen van een centraal overzicht had afgelopen jaar niet de hoogste prioriteit in de ontwikkeling van het kennisveiligheidsbeleid. Hiervoor worden verschillende verklaringen aangedragen. Ten eerste geven verschillende instituten aan dat zij geen of weinig risicovolle partnerschappen hebben. Ten tweede speelt de kleinschaligheid van instituten, waardoor alle partnerschappen in beeld zijn, ook als ze niet in een centraal overzicht met veiligheidsinformatie worden bijgehouden. Hierbij speelt bovendien dat door de kleinschaligheid er beperkte capaciteit is geweest om het overzicht in te richten in samenhang met het bredere risicomanagementsysteem.

5.1.2 Partneracceptatiebeleid (due diligence)

Zowel de KNAW als NWO-I hebben een centraal partneracceptatiebeleid. Bij de KNAW en NWO-instituten wordt deze centrale richtlijn geïmplementeerd. De beoordeling van mogelijke hoog risico-partnerschappen liggen bij beide organisaties bij het bureau en de besluitvorming bij de directie/bestuur. Overwegingen hierbij zijn het risicoprofiel van de inhoud van het onderzoek, de aard van de overeenkomst en de achtergrond van de samenwerkingspartner.

De KNAW voert sinds eind 2023 due diligence onderzoek uit naar mogelijke buitenlandse partners en opdrachtgevers met een verhoogd risicoprofiel, en heeft deze procedure opgenomen in het kennisveiligheidsbeleid. Dit risicoprofiel is breder dan alleen kennisveiligheid en gaat bijvoorbeeld ook over de rechtmatigheid van de herkomst van financiële middelen van nieuwe financiers en samenwerkingspartners. De KNAW maakt voor het risicoprofiel gebruik van software van Altares Dun en Bradstreet. Het Knowledge Transfer Office (KTO) van de KNAW is betrokken bij het due diligence proces voor juridische expertise. Eventueel wordt het Loket geconsulteerd voor extra zekerheid.

Bij partnerschappen die als hoog risicovol worden beoordeeld ligt de verantwoordelijkheid voor aangaan van de samenwerking bij de directie van de KNAW. Voor andere partnerschappen ligt de verantwoordelijkheid bij de instituutsdirecteur. Bij de KNAW-instituten is het bewustzijn rondom samenwerking gegroeid, maar dat bewustzijn is breder dan alleen kennisveiligheid. Het gaat hier bijvoorbeeld ook over samenwerking met de fossiele industrie.

Het NWO-I-bureau heeft een richtlijn voor het uitvoeren van due diligence naar de achtergrond van buitenlandse partners. NWO-I heeft hierbij nog geen specifieke juridische of veiligheidsexpertise geïmplementeerd. Het adviesteam kennisveiligheid is altijd beschikbaar, en via de coördinator kennisveiligheid kan het Loket geraadpleegd worden als dit soort kennis wel nodig is. Volgens de richtlijn van NWO-I wordt de samenwerking beoordeeld op de mate waarin het onderwerp van de samenwerking en de achtergrond van de partner als risicovol worden gezien. De verantwoordelijkheid voor het aangaan van partnerschappen is nog niet formeel vastgesteld door het NWO-I-bestuur. Informeel ligt die verantwoordelijkheid momenteel in eerste instantie decentraal bij de instituutsdirecteur. Bij een hoog risico moet het stichtingsbestuur de samenwerking goedkeuren, dit nieuwe beleid moet nog formeel worden vastgelegd.

5.1.3 Voorkomen van financiële afhankelijkheid

Financiële afhankelijkheid ontstaat wanneer onderzoek afhankelijk is van financiering vanuit een andere partij, die daarmee (in theorie) de mogelijkheid verkrijgt om het onderzoek te beïnvloeden.
De KNAW heeft geen concreet beleid om dit te voorkomen. Wel geeft de KNAW aan dat men werkt aan bewustzijn binnen de instituten om financiële afhankelijkheid te voorkomen. Ook NWO-I heeft naast de

hierboven genoemde richtlijn voor het aangaan van samenwerking geen specifiek beleid voor het voorkomen van financiële afhankelijkheid. Een NWO-instituut geeft aan beleid om te voorkomen dat ze in de positie van financiële afhankelijkheid komen. De overige NWO-instituten hebben geen specifiek beleid, omdat de voorwaarden voor ongewenste financiële afhankelijkheid niet aanwezig zijn.

5.1.4 Voorkomen automatische verlenging

De Leidraad geeft aan dat het niet wenselijk is om lopende samenwerkingsverbanden automatisch te verlengen zonder beoordeling of deze samenwerking nog steeds wenselijk is. Dit is belangrijk om te voorkomen dat mogelijk nieuwe risico's in lopende samenwerkingen niet opgemerkt worden. De KNAW heeft hier momenteel geen beleid voor, bij NWO-I ligt dit beleid bij de instituten.
De twee NWO-instituten die hierop beleid hebben, voeren dit via hun contractenregister, waarin alle contracten staan. Dit register geeft geautomatiseerde meldingen als de einddatum van een contract in zicht komt. Zes NWO-instituten hebben geen beleid en één instituut vind het niet van toepassing.
Eén NWO-instituut geeft aan hier in te toekomst strakker op te willen sturen, zeker bij grote onderzoeksconsortia. Een ander instituut heeft geen formele procedure, maar geeft aan dat het informeel beleid is dat samenwerkingen nooit stilzwijgend verlengd worden omdat deelname aan een aflopende samenwerking altijd een expliciet moment is. Tenslotte geeft een instituut aan geen formeel beleid te hebben omdat ze enkel samenwerkt via onderzoeksprojecten, die per definitie eindig zijn.

5.2 Juridische kaders en gedragscodes

5.2.1 Compliance met EU-exportcontrole van dual-use-technologie

Dual-use-goederen zijn producten, diensten en technologieën die zowel voor civiele als militaire doeleinden kunnen worden gebruikt. Voor de export van dual-use technologieën zijn gedetailleerde EU-export regels opgesteld. Deze zijn onderverdeeld in de categorieën nucleaire goederen, speciale materialen en aanverwante apparatuur, materiaalverwerking, elektronica, computers, telecommunicatie en informatiebeveiliging, sensoren en lasers, navigatie en vliegtuigelektronica, zeewezen en schepen, en ruimtevaart en voortstuwing.

Bij het KNAW-bureau is een paragraaf over export controle van dual-use technologie opgenomen in het kennisveiligheidsbeleid. Momenteel ligt de verantwoordelijk bij de KNAW-instituten om te bepalen of een technologie dual-use is. Het KNAW-bureau geeft aan dat dit vanwege het lage TRL-niveau nauwelijks aan de orde is.

De meeste KNAW- en NWO-instituten geven aan dat exportcontroles niet relevant zijn omdat het verrichtte onderzoek een te laag TRL-niveau heeft om dual-use te zijn en instituten überhaupt geen fysieke producten exporteren.

Voor een aantal instituten is deze regelgeving echter wel relevant. Zij hebben de naleving daarvan op verschillende manieren geborgd. Twee instituten gebruiken de conceptlijst met sensitieve technologieën van het ministerie van OCW om te bepalen of een technologie *dual-use* toepassingen heeft. Twee andere instituten maken gebruik van de Douane om te controleren of een product geëxporteerd kan worden. Een ander instituut geeft aan bij export binnen en buiten de EU gebruik te maken van externe expertise, en dat door ervaringen uit het verleden de interne expertise ook toeneemt.

5.2.2 Compliance met niet-EU import- en exportregels

Ook landen buiten de EU hebben import- en exportregels die voor de KNAW en NWO-I relevant kunnen zijn. Ook hier geven veel instituten aan dat deze regels voor hen niet spelen, omdat zij geen producten of technologieën im- of exporteren. Enkele instituten melden dat de doorverkoop van Amerikaanse apparatuur contractueel niet is toegestaan, waardoor zij verder beleid niet nodig achten.

Bij instituten waar deze regels wel spelen is compliance op verschillende manieren geborgd, en veelal op deze manier als EU-exportregels. Een instituut borgt dit via de juridische afdeling, een ander instituut betrekt de Douane bij de im- en export van producten, en weer een ander instituut huurt indien nodig externe expertise in. Het laatste instituut im- of exporteert zelf geen producten, maar is actief in internationale netwerken waardoor deze regels soms relevant worden.

5.2.3 Compliance met internationale en EU-sanctieregimes

Het KNAW-bureau geeft aan dat de instituten zich bewust zijn van EU-sanctieregimes. Er worden geen gesanctioneerde kennis of goederen gedeeld met Iran, en met Rusland wordt überhaupt niet meer samengewerkt.

Op instituutsniveau zeggen meerdere instituten van de KNAW en NWO-I beleid rondom compliance niet van toepassing te vinden. Veel instituten geven aan geen transacties te doen of partnerschappen te hebben met landen die onder sanctieregimes vallen. Twee instituten geven wel aan dat de verantwoordelijkheid voor compliance expliciet bij de instituutsmanager en het MT ligt.

5.2.4 Gedragscodes

Gedragscodes zijn niet-bindende richtinggevende richtlijnen die kennisinstellingen kunnen helpen bij het maken van afwegingen. Voorbeelden hiervan zijn de Leidraad, het Kader Kennisveiligheid Universiteiten[28] en de EU guidelines on Tackling R&I foreign interference[29]. Sommige instituten noemen zelf hier ook de Nederlandse Gedragscode Wetenschappelijk Integriteit[30] als belangrijke richtlijn.

Het KNAW-bureau deelt dit soort gedragscodes via intranet en in werkgroepen, maar heeft weinig zicht op de daadwerkelijke toepassing ervan binnen instituten. De meeste instituten van de KNAW geven aan deze gedragscodes niet toe te passen in relatie tot kennisveiligheid, waarbij sommige instituten toelichten dat dit ook niet relevant is in hun werkveld. Bij de NWO-instituten worden gedragscodes op instituutsniveau toegepast en zijn deze verwerkt in centrale richtlijnen van NWO-I.

[28] VSNU Kader Kennisveiligheid Universiteiten.pdf (universiteitenvannederland.nl)
[29] Tackling R&I foreign interference - Publications Office of the EU (europa.eu)
[30] Nederlandse gedragscode wetenschappelijke integriteit - KNAW

5.3 Dilemma's en aandachtspunten

Op het vlak van internationale partnerschappen en juridische kaders speelt een aantal dilemma's en aandachtspunten.

Het is een dilemma om een goede balans te vinden tussen kennisveiligheid en de principes van *open science*. Dit dilemma wordt op meerdere manieren concreet. Zo is het voor onderzoekers lastig om te bepalen of ze samen kunnen publiceren met onderzoekers uit landen met een verhoogd risicoprofiel. Dit is geen formeel partnerschap, maar wel een vorm van samenwerking. Ook kan de beoordeling van samenwerkingspartners leiden tot discriminatie van personen uit bepaalde landen.

Daarnaast zijn sommige instituten actief in multilaterale samenwerkingsverbanden op Europees niveau. Binnen dit soort programma's wordt soms Europees besloten om de samenwerking met risicovolle of gesanctioneerde landen voort te zetten. Dit kan ingaan tegen het Nederlandse beleid.

Ten slotte worstelen instituten met de scope van *due diligence. Due diligence* richt zich meestal op de potentiële onderzoekspartner, maar relaties van deze partner kunnen ook een risico vormen. Ook werken de KNAW en NWO-instituten samen met landen die niet direct als risicovol worden gezien, maar wel in de invloedssfeer zitten van landen die dat wel zijn. Het is een dilemma of deze aspecten ook onderdeel moet zijn van *due diligence*, want het kan het proces onnodig tijds- en middelenintensief maken.

5.4 Lessons learned

Uit de analyse komen twee lessen rondom internationale partnerschappen en juridische kaders naar voren.

Ten eerste, de KNAW- en NWO-instituten hebben behoefte aan meer helderheid in de kaders rondom kennisveiligheid. Instituten zoeken bijvoorbeeld naar een heldere checklist die afdwingt dat iedere betrokkene voorafgaand aan een onderzoek (bij het schrijven van projectvoorstellen of financieringsaanvragen) over kennisveiligheidsrisico's nagedacht heeft. Dit heeft enige spanning met de Leidraad, waarin staat dat kennisveiligheidsrisico's zich slecht laten vatten in checklists, en dat die een gevaar van schijnveiligheid hebben.

Ten tweede werken instituten onderling veel samen. Instituten zijn soms te klein om zelf alle relevante expertise in huis te hebben. Uitwisseling waarbij specialistische expertise tussen instituten gedeeld kan worden kan daarbij helpen. De bureaus van de KNAW en NWO-I ondersteunen de instituten hierbij.

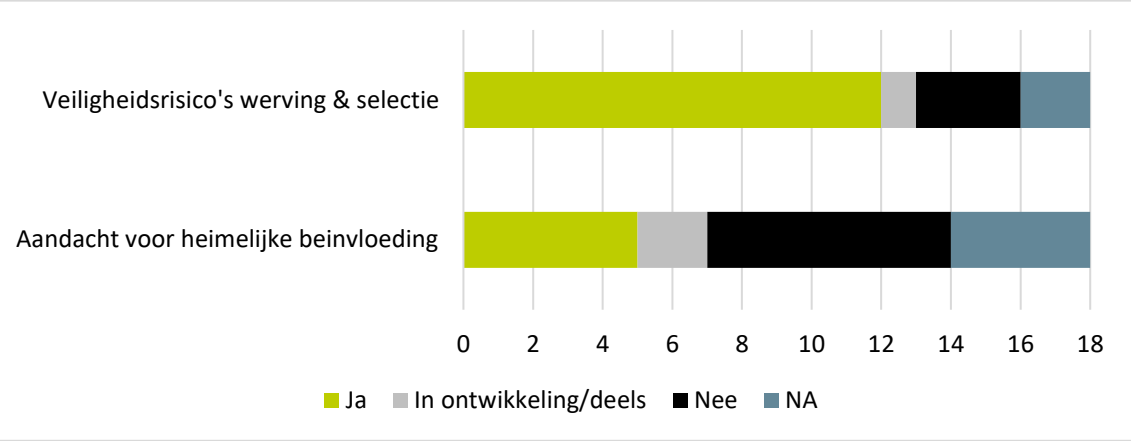
6 Personeelsbeleid

De Leidraad stelt dat het wenselijk is dat kennisveiligheid onderdeel wordt van het personeelsbeleid. In dit hoofdstuk beschrijven we eerst op welke manier kennisveiligheid op dit moment is geïmplementeerd in verschillende onderdelen van het personeelsbeleid van de instituten. In lijn met de Leidraad verstaan we personeelsbeleid hier als het beleid rondom overzichten van (gast)werknemers, rondom de werving en selectie van nieuw personeel en rondom (heimelijke) beïnvloeding van de diaspora door statelijke actoren. Daarna bespreken we welke dilemma's en aandachtspunten hierbij naar voren komen en de lessen die de instellingen op dit vlak hebben geleerd.

6.1 Vertaling kennisveiligheid in personeelsbeleid

De meerderheid van de KNAW- en NWO-instituten (15 van de 18) ontwikkelt of heeft al aandacht voor kennisveiligheid als onderdeel van het personeelsbeleid (zie eerder Tabel 2.1). Figuur 6.1 geeft een overzicht van kennisveiligheidsactiviteiten rondom personeelsbeleid van de instituten.

Figuur 6.1 Overzicht activiteiten personeelsbeleid (n=18)



6.1.1 Overzicht (gast)werknemers

De KNAW- en NWO-I-bureaus zijn gevraagd of zij een centraal en up-to-date overzicht bijhouden van werknemers, gasten en gastwerknemers die een risico vormen op het gebied van kennisveiligheid. De KNAW geeft aan een dergelijk overzicht bij te houden, maar hier niks mee te doen, omdat zij niet willen discrimineren op basis van nationaliteit. Het NWO-I geeft aan geen centraal overzicht bij te houden, maar heeft wel een quick-scan uitgevoerd in 2022 om hier zicht op te krijgen.

6.1.2 Werving en selectieprocedure

Twee derde van de instituten (12 van de 18) geeft aan veiligheidsrisico's in meer of mindere mate mee te wegen bij de werving en selectie van nieuwe medewerkers. Deze instituten voeren cv-checks uit, laten een screening en/of toetsing door het Loket Kennisveiligheid uitvoeren, vragen om een Verklaring Omtrent het Gedrag (VOG), of voeren zelf een (globale) check uit op de connecties met landen met een verhoogd risicoprofiel. Twee instituten geven aan dat zij alleen om een VOG vragen bij bepaalde functies. Vijf instituten geven expliciet aan dat zij per kandidaat bekijken of uitgebreidere screeningsmaatregelen noodzakelijk zijn. Instituten zetten uitgebreidere screeningsmaatregelen bijvoorbeeld in voor kandidaten afkomstig uit landen met een verhoogd risicoprofiel. Zowel uit de

verdiepende gesprekken als de zelfevaluatie blijkt dat de interpretatie van het begrip 'screening' sterk varieert per instituut. Sommige instituten laten de screening uitvoeren door de AIVD, terwijl andere instituten een controle van het cv als screening beschouwen.

Zes instituten geven aan dat zij veiligheidsrisico's niet of nauwelijks meenemen in de werving en selectie van nieuwe medewerkers. Twee van deze instituten geven hiervoor als onderbouwing dat de werkvelden waarin ze actief zijn geen kennisveiligheidsrisico's met zich meebrengen.

KNAW-instituten dienen altijd bij het bureau melding te doen bij twijfels over een sollicitant. De coördinator kennisveiligheid van de KNAW kijkt vervolgens mee met de gesignaleerde risico's en schakelt indien nodig met het Loket Kennisveiligheid. Voor de NWO-instituten geldt dat er iedere drie weken een HR-overleg plaatsvindt. Ook vindt een maandelijks NWO-I-breed kennisveiligheidsoverleg plaats. Voor beide overleggen geldt dat NWO-instituten casuïstiek kunnen inbrengen.

Betrokkenen van één instituut geven aan dat HR-medewerkers op dit moment nog onvoldoende toegerust zijn op het herkennen van kennisveiligheidsrisico's in de sollicitatieprocedure. In 2024 staat een bewustzijnscampagne gepland die het (HR-)personeel moet helpen bewuster te maken van de kennisveiligheidsrisico's.

6.1.3 Heimelijke beïnvloeding

Onderdeel van het thema kennisveiligheid is de aandacht voor (heimelijke) beïnvloeding van de diaspora door statelijke actoren, bijvoorbeeld medewerkers die onder druk of invloed staan van de eigen overheid.

De aandacht voor heimelijke beïnvloeding is beperkt binnen de KNAW- en NWO-instituten. Het begrip kennisveiligheid wordt binnen de instituten vaak primair geassocieerd met het weglekken van gevoelige (dual-use) kennis en technologieën.
Het merendeel van de instituten (17 van de 18) geeft aan geen specifiek beleid te hebben vastgelegd voor de bescherming tegen aantasting van sociale veiligheid als gevolg van (heimelijke) beïnvloeding. Een aantal van deze instituten licht hun antwoord toe. Zij geven aan dat beïnvloeding door statelijke actoren niet lijkt voor te komen bij hun medewerkers omdat zij niet samenwerken met landen met een verhoogd risicoprofiel en/of omdat er geen medewerkers met CSC-beurzen bij het instituut worden aangenomen. Een derde van de instituten geeft aan dat zij geen formeel beleid hebben vastgelegd, maar wel aandacht hebben voor het onderwerp. Zij bekijken bijvoorbeeld op case-by-case basis of meer aandacht en/of interventies omtrent heimelijke beïnvloeding nodig zijn.

Eén instituut geeft in de toelichting nadrukkelijk aan wel beleid te hebben voor (heimelijke) beïnvloeding van de diaspora door statelijke actoren. Dit instituut voert persoonlijke gesprekken met medewerkers uit landen met een verhoogd risicoprofiel die betrokken zijn bij onderzoek dat valt onder de kroonjuwelen. Het instituut bespreekt met hen politieke ontwikkelingen en neemt, indien nodig, (aangepaste) maatregelen wanneer medewerkers uit landen met een verhoogd risicoprofiel van plan zijn terug te reizen naar het land van herkomst.

Uit de verdiepende gesprekken met de instituten maken we op dat men zich wel breder bewust is van de risico's omtrent heimelijke beïnvloeding. Zo benadrukt een van de betrokkenen van de instituten dat het risico op heimelijke beïnvloeding voor hun instituut niet beperkt blijft tot medewerkers uit landen met een hoog risicoprofiel, maar zich ook uitstrekt tot medewerkers uit andere landen. Het

managementteam van dit instituut neemt deze risico's regelmatig in overweging tijdens hun besprekingen.

6.2 Dilemma's en aandachtspunten

Een aantal instituten geeft aan tegen dilemma's rondom personeelsbeleid aan te lopen. In deze paragraaf bespreken we de dilemma's en aandachtspunten die we in de gesprekken en de ingevulde vragenlijsten het meest terug horen.

6.2.1 Achtergrondtoetsing[31]

Verschillende instituten geven aan het goed beoordelen van de achtergrond van nieuw personeel ingewikkeld te vinden. Meerdere betrokkenen betwijfelen of een eigen achtergrondtoetsing of screening (zeker zonder inmenging van overheidsdiensten) wel voldoende dekkend is. Een ander instituut benoemt juist niet een overmatig voorzichtige benadering te willen hanteren voor nieuwe medewerkers. Ook zoeken meerdere instituten naar handvatten, onder meer voor de beoordeling van risico's op basis van achtergrond en opleidingshistorie van sollicitanten, bijvoorbeeld als dit gaat om het verschil tussen hebben gewoond in een land met een verhoogd risicoprofiel of hebben gewerkt bij een risicovolle instelling in een dergelijk land.

Instituten geven aan dat een goede toetsing van de achtergrond van nieuw personeel tijdsintensief is. Een vertraagde sollicitatieprocedure zou volgens hen potentiële sollicitanten sterk ontmoedigen om binnen Nederland te solliciteren. Dit kan op termijn een negatieve impact hebben op de wetenschappelijke positie van Nederland. Screeningsbeleid op Europees niveau zou dit probleem volgens de instituten kunnen voorkomen. Meerdere instituten geven aan dat de huidige screening vanuit de veiligheidsdiensten en het beantwoorden van vragen rondom een sollicitant door het Loket Kennisveiligheid te traag verloopt. Ook geven twee instituten aan dat de antwoorden door het Loket op hun vragen te algemeen of te onduidelijk waren.

6.2.2 CSC-promovendi

Uit de zelfevaluatie en de verdiepende gesprekken valt op te maken dat zowel de instituten als de bureaus zoekende zijn in het al dan niet aannemen van studenten met een CSC-beurs.[32] Zowel de KNAW als NWO-I voeren gesprekken over dit thema maar hebben nog geen centraal beleid omtrent het al dan niet accepteren van CSC-promovendi.

Een deel van de instituten geeft aan zelf de keuze te hebben gemaakt om geen studenten met CSC-beurzen meer aan te nemen. Zij hebben deze beslissing bijvoorbeeld genomen omdat zij vermoeden dat deze groep te maken heeft met een verhoogd risico op heimelijke beïnvloeding en omdat de studiebeurs vanuit de Chinese overheid promovendi niet voorziet in een toereikend salaris. Een van de instituten vermeldt dat de beslissing om geen CSC-promovendi meer aan te nemen relatief eenvoudig was, aangezien het binnen dit instituut om slechts een beperkt aantal gevallen gaat en het stopzetten van de acceptatie van dit type promovendi geen verdere impact heeft op de bedrijfsvoering. Een ander

---

31 Instituten hanteren zowel in het vragenlijstonderzoek als in de verdiepende gesprekken consequent de term 'screenen' wanneer zij spreken over het uitvoeren van achtergrondonderzoek naar (nieuw) personeel, ongeacht wie het uitvoert. In dit rapport hanteren wij de term '(achtergrond)toetsing' als het gaat om screening door de instelling zelf. De term 'screening' gebruiken we alleen voor screening uitgevoerd door de veiligheidsdiensten/Rijksoverheid of wanneer we spreken over het (concept) wetsvoorstel Screening Kennisveiligheid.

32 Recent is een studie door Clingendael verschenen die dieper ingaat op dit specifieke thema.

instituut geeft daarentegen aan dat CSC-promovendi van grote waarde zijn voor het onderzoek dat binnen het instituut wordt uitgevoerd en dat de kennisveiligheidsrisico's zeer gering zijn. Enkele instituten zouden daarom graag blijven werken met CSC-promovendi.

6.2.3 Discriminatie

Instituten geven nadrukkelijk aan niet te willen discrimineren en te allen tijde te willen voorkomen dat medewerkers zich niet meer welkom voelen binnen de organisatie. Een van de instituten illustreert dit door te verklaren dat ze geen sollicitanten willen afwijzen puur vanwege hun afkomst uit Rusland of China. Betrokkenen van dit instituut geven aan dat de uiteindelijke beslissingsbevoegdheid over het al dan niet aannemen van een sollicitant uit een land met 'een verhoogd risicoprofiel altijd bij het instituut zelf moet blijven liggen.

Meerdere instituten zoeken naar richtlijnen om adequaat om te gaan met medewerkers of studenten afkomstig uit landen met een verhoogd risicoprofiel. Een instituut benadrukt bijvoorbeeld het belang van het stellen van de juiste (non-discriminatoire) vragen tijdens sollicitatiegesprekken. Ook benoemt het instituut dat het ingewikkeld is om kennisveiligheidsrisico's met medewerkers uit bepaalde landen te moeten bespreken. Betrokkenen van dit instituut geven aan dat ze moeite hebben om de mogelijk negatieve impact van dergelijke gesprekken op de medewerkers correct in te schatten.
Betrokkenen van een ander instituut geven in de verdiepende gesprekken aan zich bewust te zijn van het risico op discriminatie. Bij dit instituut krijgen studentmedewerkers uit landen met een verhoogd risicoprofiel bijvoorbeeld geen account om binnen de instituutsomgeving in te loggen en wordt hen geen toegangspasje verstrekt. Dergelijke keuzes vragen volgens de betrokkenen van dit instituut om uitleg. Het instituut probeert dit op een zo tactisch mogelijke manier te doen, maar geeft aan dat deze gesprekken soms zeer complex zijn.

In de verdiepende gesprekken benadrukken meerdere betrokkenen (van zowel de instituten als een van de bureaus) dat de focus vanuit de Rijksoverheid mogelijk te beperkt is op de vier landen met een verhoogd risicoprofiel (Iran, Noord-Korea, Rusland en China). Ze stellen dat ook landen buiten deze categorie risico's kunnen opleveren.

6.3 Lessons learned

Uit de analyse komen twee lessen rondom personeelsbeleid naar voren. Ten eerste, een van de instituten heeft aandacht voor kennisveiligheid opgenomen in hun sollicitatieprocedure, waarbij al in een vroeg stadium voor iedere sollicitant een risicoprofiel wordt opgesteld op basis waarvan passende maatregelen worden genomen. In gevallen waarbij sprake is van een hoog risicoprofiel wordt er een formele controle uitgevoerd door de instituutsmanager. Doordat het risicoprofiel al in een vroeg stadium van de sollicitatieprocedure wordt opgesteld, hoeven er geen kennisveiligheidsrisico's meer te worden afgewogen wanneer een kandidaat eenmaal is geselecteerd.

Ten tweede, drie instituten geven aan alle nieuwe medewerkers, ook uit landen zonder een verhoogd risicoprofiel, bij hun aanstelling te vragen een geheimhoudingsverklaring of *confidentiality agreement* te tekenen, waarin zij zich committeren aan het vertrouwelijk behandelen van gevoelige informatie. Dit draagt volgens betrokkenen bij aan versterkt bewustzijn onder medewerkers dat zij in aanraking kunnen komen met vertrouwelijke gegevens, die niet gedeeld mogen worden met derden.

7 Conclusie en aandachtspunten

In dit hoofdstuk geven we een beknopte hoofdconclusie ten aanzien van het sectorbeeld kennisveiligheid onderzoeksinstituten KNAW en NWO-I, namelijk dat het beleid nog in ontwikkeling is, maar dat betrokkenen beperkt risico's zien. Daarnaast concluderen we dat de onderzoeksinstituten en bureaus tegen een aantal dilemma's aanlopen die van invloed zijn op de ontwikkeling van het kennisveiligheidsbeleid. Tot slot presenteren we een aandachtspunt voor de verdere ontwikkeling van het nationale kennisveiligheidsbeleid.

7.1 Conclusie: beleid in ontwikkeling, betrokkenen zien beperkt risico's

Het belang van het kennisveiligheidsbeleid is bij zowel KNAW als NWO-I in een stroomversnelling geraakt door de ontwikkeling en publicatie van de Leidraad en de oproep van de minister om een risicoanalyse uit te voeren. Het belang van kennisveiligheidsbeleid wordt door de diverse instituten verschillend ervaren, waarbij de bureaus en instituten over het algemeen beperkt risico's zien op het vlak van kennisveiligheid.

De instituten zijn beperkt van omvang, variërend van enkele tientallen tot enkele honderden (minder dan 400) medewerkers. Bovendien zijn instituten onderverdeeld in onderzoeksgroepen met groepsleiders. Hierdoor zijn de 'lijntjes' binnen de instituten vaak kort, betrokkenen op het gebied van kennisveiligheid weten elkaar binnen en tussen instituten goed te vinden en zijn snel bewust van casuïstiek. Het persoonlijke contact helpt om vervolgens op een goede manier met deze casussen om te gaan. Waar de bureaus toezien op het vaststellen van formeel beleid, kiezen veel instituten er daarom voor om op instituutsniveau het beleid op meer informele wijze te implementeren. Doordat de instituten beperkt zijn in omvang, zijn zij bovendien gedwongen om veel met elkaar samen te werken op kennisveiligheidsbeleid. De adviesteams zijn gepositioneerd in samenwerking tussen de instituten op de meer centrale niveaus van KNAW of NWO-I. Deze worden bovendien ondersteund door de coördinatoren van de bureaus.

De NWO-instituten voeren in grote mate technologisch onderzoek uit. Voor verschillende instituten geldt dat zij al langer bewust zijn van de gevoeligheid van hun onderzoek en hier beleid op voeren. Een nuancering die ze daarbij aangeven, is dat zij voornamelijk fundamenteel onderzoek uitvoeren op een laag TRL-niveau (0-1), waardoor er beperkte risico's zijn op kennisveiligheid. Er is veel samenwerking en afstemming tussen de NWO-instituten en de ondersteuning vanuit het NWO-I-bureau wordt ervaren als vrij intensief. Er is dus ruime aandacht voor kennisveiligheid, hoewel dit als arbeidsintensief wordt ervaren.
De KNAW-instituten zijn vaker gericht op sociaal- of geesteswetenschappelijk onderzoek, waar sensitieve technologie en exportbeperkingen niet spelen. Meerdere instituten geven aan dat zij daarom beperkt te maken hebben met kennisveiligheidsvraagstukken. Dit is opvallend, omdat de KNAW in een *position paper* eerder adviseerde "differentieer steeds tussen de drie verschillende betekenissen van kennisveiligheid."[33] Een aantal instituten geeft aan dat zij voornamelijk risico's zien op ongewenst gebruik van hun data, wat reeds de aandacht krijgt in hun beleid op informatiebeveiliging. Het debat over ethische vragen rondom samenwerkingspartners en financieringen gaat momenteel breder over

[33] KNAW (2023). Kennisveiligheid - KNAW position paper, p. 2.

zowel de samenwerking met de fossiele industrie als over samenwerking met (partners uit) bepaalde landen.

De KNAW- en NWO-instituten hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel 2.1).[34] Daarbij zien we een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad:

- Beleid op fysieke en digitale bescherming is vaker vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid.
- Beleid op (risicovolle) internationale partnerschappen is bij de KNAW en NWO-I op het niveau van de bureaus vastgesteld met aantoonbare uitvoering. Daarnaast is de implementatie van het beleid uitgevraagd bij de NWO-instituten, die in verschillende fases van beleidsimplementatie zitten.[35]
- Beleid op toepassing van juridische kaders (voor compliance met export controle en sanctieregimes) ontbreekt relatief vaker dan de andere onderdelen in het kennisveiligheidsbeleid.
- De vertaling van kennisveiligheid in het personeelsbeleid is bij de meerderheid van de instituten vastgesteld met aantoonbare uitvoering.

Tabel 7.1. Zelfscores op fase van beleidsontwikkeling. (een aantal instituten heeft op één of meer onderdelen geen score ingevuld. Hierdoor verschilt de n per onderwerp)

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en uitvoering aantoonbaar	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig
Risicoanalyse	1	6	6	3	2	
Risicomanagement	1	6	3	5	1	2
Fysieke en digitale beschermings-maatregelen	1	2	2	9	2	2
Internationale partnerschappen (NWO-instituten)	1	2	2	2		
Juridische kaders	7	1		5	1	
Personeelsbeleid	3	3	2	7		3

De risicoanalyses (het continu inschatten van risico's bij nieuwe samenwerkingen, werknemers, inkomende gasten, etc.) zijn bij zowel de KNAW als NWO-I volledig bij de instituten belegd, de bureaus hebben zichzelf hier niet op gescoord. Op de overige onderdelen geldt voor NWO-I dat beleid deels nog in ontwikkeling is en deels is vastgesteld. Bij de KNAW is beleid veelal (deels) vastgesteld, met uitzondering van het personeelsbeleid dat nog in ontwikkeling is. Ook staat bij de KNAW de komende periode een bewustwordingscampagne gepland.

[34] Deze rubric is afgeleid van de volwassenheidsniveaus zoals die worden gebruikt in bijvoorbeeld het SURFaudit toetsingskader IBHO, het toetsingskader MBO Digitaal en toetsingskader PO-VO Kennisnet. De rubric is eerder ook toegepast in het sectorbeeld universiteiten.

[35] Dit is niet uitgevraagd bij de individuele KNAW-instituten.

7.2 Dilemma's

In het ontwikkelen en uitvoeren van kennisveiligheidsbeleid zien we een aantal dilemma's en aandachtspunten bij de onderzoeksinstituten en bureaus van de KNAW en NWO-I die van belang zijn voor het landelijke debat over kennisveiligheidsbeleid.

7.2.4. Voorkomen stigmatisering en discriminatie

De KNAW en NWO-I uiten zorgen over stigmatisering en discriminatie, of een cultuur van uitsluiting. Als het gaat over samenwerkingen met instellingen of onderzoekers uit specifieke landen ligt stigmatisering snel op de loer. Abstract nationaal beleid vertaalt zich binnen de instellingen tot impact op het individuele niveau van veelbelovende sollicitanten en gewaardeerde collega's, wat betrokkenen binnen instellingen (onderzoekers, bestuurders en HR) in een lastige positie plaatst. Sommige instituten nemen het zekere voor het onzekere, en werken bijvoorbeeld helemaal niet meer samen met instituten uit Rusland, China en Iran. Deze nauwe focus is een risico omdat samenwerkingen en werknemers uit andere landen ook risico's met zich kunnen meebrengen.

7.2.1 Focus op technologisch onderzoek en proportionaliteit

Het kennisveiligheidsbeleid is in de praktijk in sterke mate gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie. De relevantie en proportionaliteit van kennisveiligheidsbeleid is daarom punt van discussie voor instituten die in de regel geen nieuwe technologie ontwikkelen of fundamenteel onderzoek doen. Meerdere instituten geven aan dat ze inschatten een **laag risicoprofiel** te hebben, omdat ze geen technologisch onderzoek doen of omdat technologisch onderzoek op het laagste TRL-niveau plaatsvindt. Hierdoor vragen ze zich tot op welke hoogte het nodig en proportioneel is om kennisveiligheidsbeleid en procedures te implementeren en onderhouden. Kennisveiligheidsbeleid, vastgelegde processen en protocollen kunnen helderheid scheppen voor het signaleren en mitigeren van kennisveiligheidsrisico's. KNAW en NWO-I en hun instituten geven echter tegelijkertijd aan dat het beleid niet moet leiden tot een **niet-proportionele bureaucratie** om risico's te beperken.

7.2.2. Academische waarden

Kennisveiligheid introduceert een nieuwe balans waarin keuzes moeten worden gemaakt tussen academische kernwaarden en nationale veiligheid. KNAW en NWO-I onderstrepen het belang van internationale samenwerking, autonomie en academische vrijheid als randvoorwaarden voor excellent onderzoek. Wetenschappelijke instituten zijn van oudsher gericht op kennisdeling, zowel binnen als buiten de instelling, en hebben traditioneel weinig structuren om kennis juist te beschermen. Ook geven enkele instituten aan onduidelijkheid te ervaren hoe het kennisveiligheidsbeleid zich dient te verhouden tot het overheidsbeleid naar meer open science, wat juist moet leiden tot meer toegankelijkheid van wetenschappelijke kennis.

7.2.3. Het instituut als toegangspoort

Risicoanalyses zijn in sterke mate gericht op het interne risicoprofiel van kennisgebieden, faciliteiten en medewerkers. Een vraag is echter in welke mate het *externe* risicoprofiel van instituten moet worden meegewogen voor de kennisveiligheid van het kennisecosysteem. Sommige instituten doen zelf geen sensitief onderzoek, maar genieten wel een hoge reputatie. Deze instituten geven aan dat hun ex-werknemers, dankzij een goede referentie, zeer makkelijk binnenkomen bij werkgevers waar mogelijk wel sensitief onderzoek wordt gedaan. Vanuit dat belang vinden deze instituten het belangrijk hun risicomanagement op orde te hebben.

7.2.5. Gelijk speelveld

Ten slotte hebben veel instituten behoefte aan duidelijker nationaal en Europees beleid, inclusief duidelijke richtlijnen en tools vanuit het perspectief van de belangen en waarden van Europa. Daarbij benadrukken instituten ook het belang voor consistentie en afstemming tussen nationaal en Europees beleid. Zij zien nu nog te vaak tegenstrijdige adviezen, waar een samenwerking met een buitenlandse universiteit of bedrijf door het ene overheidsinstituut wordt afgeraden, terwijl deze wordt gestimuleerd door een ander overheidsinstituut. Zeker waar onderzoek vaak in consortia wordt uitgevoerd en op basis van Europese financiering, zien onderzoekers verschillen in de richtlijnen die landen meegeven.

7.3 Aandachtspunt

Naast dilemma's komen uit het sectorbeeld ook een aandachtspunt voor het verdere nationale kennisveiligheidsbeleid.

De KNAW en NWO-instituten hebben door het gebruik van de KWAS hun risicoanalyse in sterke mate gericht op het identificeren van kroonjuwelen. Over de definitie van wat kroonjuwelen zijn en hoe hier vervolgens kennisveiligheidsbeleid op te ontwikkelen zijn nog verschillen van inzicht. Een aandachtspunt is om een duidelijk begrippenkader te formuleren, waarover overeenstemming is onder kennisinstellingen. Dit punt was eerder al een aandachtspunt in het sectorbeeld universiteiten en in het AWTI-rapport 'Kennis in conflict' (Aanbeveling 1. Conceptualiseer: verbeter het begrip van kennisveiligheid). Het lijkt het nuttig dit te verwerken in een volgende editie van de Nationale Leidraad Kennisveiligheid en in een aangepast (bij voorkeur gezamenlijk) model voor toekomstige risicoanalyses. Aandachtspunt daarbij is het voor instellingen concretiseren van risico's op heimelijke beïnvloeding en ethische vragen rondom samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd.

Bijlage 1 Vragenlijst

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
Kennisveiligheid					
1.	Hoe wordt het begrip 'kennisveiligheid' binnen uw organisatie gedefinieerd?	X		X	
2.	Sinds wanneer is er sprake van het ontwikkelen, vaststellen of uitvoeren van beleid op kennisveiligheid aan uw organisatie?	X		X	
Risicoanalyse 2022 De minister van OCW heeft op 4 april 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren, waarbij risicovolle samenwerkingen en financieringsbronnen bijzondere aandacht verdienen.[36] In deze vragenlijst maken we onderscheid tussen deze risicoanalyse op verzoek van de minister, en risicoanalyses die uw organisatie uitvoert als onderdeel van regulier beleid (volgend blok).					
3.	Kunt u toelichten of u deze risicoanalyse heeft uitgevoerd en hoe u deze heeft vormgegeven?	X	X	X	X
4.	Heeft de oproep van de minister geleid tot nieuwe of andere activiteiten in vergelijking met eventuele risicoanalyses die uw organisatie al uitvoerde als onderdeel van het eigen kennisveiligheidsbeleid? Kunt u dit toelichten?	X	X	X	X
5.	Heeft uw organisatie bij deze risicoanalyse gebruik gemaakt van een model? Zo ja, welke en waarom (Bijvoorbeeld het Model Risicoanalyse Kennisveiligheid van UNL of de Kwetsbaarheidanalyse Spionage van de AIVD)?	X	X	X	X
6.	Heeft uw organisatie bij deze risicoanalyse gebruik gemaakt van advies van het Loket Kennisveiligheid of contact gehad met de contactpersoon van uw organisatie bij de veiligheidsdiensten?	X		X	
7.	Zijn er nieuwe risico's gesignaleerd? Zo ja, op welk vlak lagen deze? (U hoeft de risico's zelf niet te benoemen, maar kunt bijvoorbeeld aangeven of deze op het vlak lagen van risico's op ongewenste overdracht van sensitieve kennis, heimelijke beïnvloeding en inmenging van statelijke actoren of ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd)	X	X	X	X
8.	Hebben de uitkomsten van deze risicoanalyse geleid tot concrete maatregelen (u hoeft de maatregelen zelf	X	X	X	X

[36] Afschrift brief aan kennisinstellingen Nationale Leidraad Kennisveiligheid | Brief | Rijksoverheid.nl

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
	niet te noemen) en/of tot het aanpassen van het kennisveiligheidsbeleid? Waarom wel of niet?				
9.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van de risicoanalyse op verzoek van de minister?	X	X	X	X
Het inschatten van risico's De volgende vragen gaan in op de risicoanalyses die uw instituut uitvoert als onderdeel van het eigen kennisveiligheidsbeleid. Indien dit eerder niet het geval was en uw instituut alleen ervaring heeft met de risicoanalyse in reactie op de oproep van de minister kunt u onderstaande vragen voor die specifieke risicoanalyse beantwoorden.					
10.	Kunt u het huidige kennisveiligheidsbeleid van uw instituut met betrekking tot het inschatten van risico's scoren aan de hand van onderstaande rubric? • Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus		X		X
11.	Maken risicoanalyses op kennisveiligheid al langer onderdeel uit van het reguliere beleid van uw instituut (eventueel onder andere terminologie)? • Ja, dat doen we op instituutsniveau • Ja, dat doen we op het niveau van onderzoeksgroepen • Ja, dan doen we op zowel instituutsniveau als het niveau van onderzoeksgroepen • Nee, de risicoanalyse n.a.v. de oproep van de minister is onze eerste ervaring hiermee • Anders, namelijk		X		X
12.	We zijn benieuwd op welke manier uw instituut risicoanalyses voor kennisgebieden maakt. Kunt u dit aan de hand van onderstaande vragen beschrijven? a) Worden sensitieve kennisgebieden binnen uw instituut geïdentificeerd? Zo ja, wie doet dat en op welk moment vindt die analyse plaats? b) Hanteert uw instituut een eigen lijst met sensitieve kennisgebieden? Zo ja, kunt u toelichten hoe deze		X		X

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
	tot stand komt en hoe uw instituut zorgt dat deze actueel blijft? c) Op welke manier bepaalt uw instituut of onderwijs of onderzoek onder deze kennisgebieden valt? d) Brengt uw instituut daarbij de 'kroonjuwelen' in kaart? In de Leidraad wordt dit gedefinieerd als kennisgebieden waarbij kennisveiligheidsrisico's zijn verbonden aan kennisoverdracht en waarop uw instituut internationaal toonaangevend is. Zo ja, kunt u toelichten hoe dit wordt gedaan?				
13.	We zijn benieuwd op welke manier uw instituut risicoanalyses maakt voor samenwerkingen met partnerorganisaties of personen uit specifieke landen: a) Hoe doet uw instituut dat en van welke informatiebronnen wordt daarbij gebruik gemaakt? b) Zijn er de afgelopen twee jaar veranderingen in kennisveiligheidsbeleid doorgevoerd met betrekking tot de manier waarop uw instituut, onderzoekers of projectleiders de samenwerking met buitenlandse partnerorganisaties of opdrachtgevers beoordelen? Zo ja, wat is hierin veranderd en wat was hiervoor de aanleiding?		X		X
14.	Zijn er binnen uw instituut standaardprocessen die in werking treden bij een bepaald risiconiveau van het kennisgebied en/of de achtergrond van de partnerorganisatie of persoon? Zo ja, hoe zien deze standaardprocessen eruit? (bijvoorbeeld, worden de benodigde risicoanalyses en controles strikter? Komt de beslisbevoegdheid op een hoger, centraler niveau te liggen?) Zo nee, kunt u toelichten hoe uw instituut hier dan mee omgaat?		X		X
15.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van het inschatten van risico's?		X		X
Organisatie risicomanagement De volgende vragen gaan in op de organisatie van risicomanagement op het gebied van kennisveiligheid binnen uw instituut. Kennisveiligheid kan belegd zijn bij verschillende afdelingen of bij verschillende verantwoordelijken. Om een beeld te krijgen hoe instituten dit organiseren vragen we graag voor verschillende afdelingen of zij een rol spelen in het kennisveiligheidsbeleid van uw instituut.					
16.	Kunt u het huidige kennisveiligheidsbeleid van uw organisatie met betrekking tot de organisaties van het risicomanagement kennisveiligheid scoren aan de hand van onderstaande rubric?	X	X	X	X

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
	• Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus				
17.	Is er binnen uw organisatie op bestuurlijk niveau een portefeuillehouder kennisveiligheid?	X		X	
18.	Heeft uw organisatie een Adviesteam Kennisveiligheid? Kunt u achtergrond, deskundigheid en samenstelling van dit team beschrijven?	X		X	
19.	Op welke wijze wordt beleidsmatige afstemming verkregen tussen het brede kennisveiligheidsbeleid van NWO-I/KNAW en het beleid van de instituten?	X	X	X	X
20.	In welke mate spelen de ethische commissie(s) (of ethical review board) binnen uw organisatie een rol in het kennisveiligheidsbeleid? (Bijvoorbeeld: kunnen ze adviseren en/of goedkeuren over ethisch gebruik van onderzoeksresultaten?)	X		X	X
21.	Zijn er vertrouwenspersonen binnen uw instelling waar medewerkers terechtkunnen met signalen over veiligheidsrisico's?	X	X	X	X
22.	Hebben technology/knowledge transfer office(s) en accelerators/startup academies binnen uw organisatie een rol in het beleid rondom kennisveiligheid? Waarom wel of niet? (U kunt hierbij denken aan processen rondom intellectueel eigendom en samenwerkingsverbanden van academische/student startups. (Indien uw organisatie niet beschikt over een technology/knowledge transfer office of accelators/startup academies graag "n.v.t." invullen)[37]	X		X	
23.	Zijn er nog andere functionarissen of organen binnen uw organisatie betrokken bij het beleid op kennisveiligheid? Zo ja, om welke functies gaat dit en welke rol spelen zij?	X		X	

[37] Deze vraag is licht aangepast t.o.v. de vragenlijst onder universiteiten. Bij universiteiten is enkel gevraagd naar de rol van TTO/KTO's, bij hogescholen zijn hier de accelerators/startup academies aan toegevoegd om beter aan te sluiten op de werking van hogescholen.

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
24.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van de organisatie van risicomanagement op kennisveiligheid?	X	X	X	X
Fysieke en digitale beschermingsmaatregelen De volgende vragen gaan over beschermingsmaatregelen gericht op fysieke en digitale toegang binnen uw organisatie.					
25.	Kunt u het huidige kennisveiligheidsbeleid van uw organisatie met betrekking tot fysieke en digitale beschermingsmaatregelen scoren aan de hand van onderstaande rubric? • Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus	X	X	X	X
26.	Geldt er voor bepaalde ruimtes (afdelingen, gebouwen, locaties, labs) een restrictief toegangsbeleid? Zo ja, hoe wordt deze afweging gemaakt? Op welk niveau gebeurt dit? a) Hoe gaat uw instituut om met buitenlandse reisdelegaties die ruimtes met een restrictief toegangsbeleid op uw instituut bezoeken?		X		X
27.	Geldt er voor bepaalde onderzoeksgegevens en documenten een restrictief toegangsbeleid? a) Zo ja, hoe wordt deze afweging gemaakt? Op welk niveau gebeurt dit? b) Indien uw instituut met zeer sensitieve gegevens werkt: werkt uw instituut met rubricering van documenten (zoals 'vertrouwelijk' of 'geheim')?		X		X
28.	Wat is de samenhang tussen cyberveiligheidsbeleid en het kennisveiligheidsbeleid op uw instelling?	X	X	X	
29.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van fysieke en digitale beschermingsmaatregelen?	X	X	X	X
Internationale partnerschappen Hieronder vragen we in welke mate uw instituut aan verschillende beleidsmaatregelen ten aanzien van internationale partnerschappen invulling geeft en wat daarbij de overwegingen zijn.					

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
30.	Kunt u het huidige kennisveiligheidsbeleid van uw organisatie met betrekking tot internationale partnerschappen scoren aan de hand van onderstaande rubric? • Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus	X	X	X	
31.	Is er op het centrale bestuursniveau een centraal en up-to-date overzicht van veiligheidsgevoelige partnerschappen en financiering? a) Hoe wordt dit overzicht actueel gehouden?	X	X	X	
32.	Heeft uw instelling een partneracceptatiebeleid? Zo ja, kunt u deze toelichten aan de hand van onderstaande vragen? a) Zijn er interne procedures waarbij in het kader van *due diligence* de achtergrond van een buitenlandse partner of opdrachtgever wordt nagegaan? b) In hoeverre wordt daarbij juridische en veiligheidsexpertise ingeschakeld? c) Wat voor afwegingen worden gemaakt bij het definitief aangaan van de samenwerking? d) Waar ligt de verantwoordelijkheid voor het aangaan van partnerschappen?	X	X	X	
33.	Heeft uw organisatie beleid om te voorkomen dat (instituten binnen) uw organisatie in een situatie van ongewenste (financiële) afhankelijkheid van statelijke actoren kan worden gebracht? a) Zo ja, kunt dit toelichten? Hoe ziet dit beleid eruit?	X	X	X	
34.	Is er een interne procedure om ervoor te zorgen dat lopende samenwerkingen met buitenlandse partners regelmatig worden geëvalueerd en dat overeenkomsten niet stilzwijgend worden verlengd? a) Worden betrokkenen vanuit uw instituut (automatisch) gealerteerd ruim voor het verlengmoment, zodat er voldoende tijd is om de afspraken kritisch tegen het licht te houden?		X	X	

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
35.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van internationale partnerschappen?	X		X	
Juridische kaders en gedragscodes Voor kennisveiligheid gelden een aantal bestaande juridische kaders en gedragscodes. U kunt aan de hand van onderstaande vragen aangeven in hoeverre uw instituut hier mee te maken heeft en mee omgaat.					
36.	Kunt u het huidige kennisveiligheidsbeleid van uw instituut met betrekking tot juridische kaders en gedragscodes scoren aan de hand van onderstaande rubric? • Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus		X	X	X
37.	Hoe is compliance met EU-exportcontrole van *dual use*-technologie[38] geborgd binnen uw instituut? a) Hoe wordt binnen uw instituut bepaald of een technologie *dual use* is?		X	X	X
38.	Hoe is compliance met niet-EU import- en exportregels geborgd? U kunt hierbij denken aan het in- en doorverkopen van Amerikaanse apparatuur.		X	X	X
39.	Hoe is compliance met internationale en EU-sanctieregimes (bijvoorbeeld ten aanzien van Rusland of Iran) geborgd binnen uw instituut?		X	X	X
40.	Hoe worden gedragscodes zoals het Kader Kennisveiligheid Universiteiten of de EU guidelines on Tackling R&I foreign interference, of andere gedragscodes, binnen uw instituut toegepast?		X	X	X
41.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van juridische kaders en gedragscodes?		X	X	X
Personeelsbeleid De Leidraad stelt dat het wenselijk is dat veiligheidsbewustzijn onderdeel wordt van het personeelsbeleid. In onderstaande vragen beschrijven we een aantal wijzen waarop dit bewustzijn					

[38] Voor *dual-use* technologieën zijn gedetailleerde Europese exportregels opgesteld. De kennisvelden die mogelijk onder deze regels vallen zijn opgedeeld in 10 categorieën, te weten: nucleaire goederen, speciale materialen en aanverwanten apparatuur, materiaalverwerking, elektronica, computers, telecommunicatie en informatiebeveiliging, sensoren en lasers, navigatie en vliegtuigelektronica, zeewezen en schepen & ruimtevaart en voortstuwing.

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
kan worden geïmplementeerd in beleid om een beeld te krijgen hoe uw instituut hier invulling aan geeft.					
42.	Kunt u het huidige kennisveiligheidsbeleid van uw instituut met betrekking tot personeelsbeleid en gedragscodes scoren aan de hand van onderstaande rubric? • Geen beleid • Beleid is in ontwikkeling • Beleid is vastgesteld en de uitvoering is aantoonbaar • Er is een verbetercyclus aanwezig en gedocumenteerd • Er is een instituutsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus	X	X	X	X
43.	Is er op centraal bestuursniveau een centraal en up-to-date (kwantitatief) overzicht van werknemers, gasten en gastwerknemers die een risico vormen op het gebied van kennisveiligheid? Waarom wel of niet?	X		X	
44.	Worden bij de werving en selectie van nieuwe medewerkers veiligheidsrisico's meegewogen? Zo ja, hoe? Is er bijvoorbeeld een interne procedure om potentiële risico's bij kandidaten tijdig te onderkennen?		X		X
45.	Hoe wordt er binnen uw instituut voor gezorgd dat HR-medewerkers veiligheidsbewust zijn (en in staat zijn om signalen die wijzen op een verhoogd risico op te pikken)?		X		X
46.	In hoeverre voert uw instituut actief beleid om een open veiligheidscultuur te creëren? a) Worden er bewustwordingscampagnes rond kennisveiligheid gevoerd? Zo ja, op welke doelgroepen richten deze campagneactiviteiten zich specifiek? b) Krijgen (nieuwe) medewerkers informatie en training om hen veiligheidsbewust te maken? c) Zijn er opfrismodules voor zittende medewerkers? d) Zijn er speciale trainingsprogramma's gericht op academische kernwaarden voor gastonderzoekers uit landen met een verhoogd risicoprofiel?		X		X

	Vraag	NWO-I bureau	NWO-instituten	KNAW bureau	KNAW instituten
47.	Beschikt uw instituut over een specifiek beleid voor dienstreizen naar landen met een verhoogd risicoprofiel? Zo ja, kunt u dit kort beschrijven?		X	X	
48.	Is er specifiek aandacht en beleid voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding van de diaspora door statelijke actoren? (Bijvoorbeeld: medewerkers afkomstig uit China die onder druk of invloed staan van de Chinese overheid) Zo ja, kunt u dit kort beschrijven?		X		X
49.	Heeft u verder nog opmerkingen of een toelichting ten aanzien van personeelsbeleid?	X	X	X	X
Evaluatie en doorontwikkeling Kennisveiligheid is een relatief nieuw onderwerp dat nog sterk in ontwikkeling is. Met onderstaande vragen kunt u dit perspectief voor uw instituut schetsen.					
50.	Wat zijn de belangrijkste dilemma's en vraagstukken voor uw organisatie bij het vormgeven van kennisveiligheidsbeleid?	X	X	X	X
51.	Heeft uw organisatie voor het komend jaar voornemens voor het (door)ontwikkelen van kennisveiligheidsbeleid in uw organisatie? Zo ja, welke voornemens zijn dat?	X		X	
52.	Wordt het beleid, procedures, en maatregelen op het gebied van kennisveiligheid binnen uw organisatie geëvalueerd? Zo ja, gebeurt dit op structurele basis? Wie zijn hierbij betrokken?	X		X	
Afsluiting					
53.	Zijn er onderdelen van uw kennisveiligheidsbeleid die hierboven niet aan bod zijn gekomen? Zo ja, dan kunt u deze hier kort noemen.	X	X	X	X
54.	Als u opmerkingen over het onderzoek of suggesties om deze vragenlijst te verbeteren heeft, dan kunt u die hieronder kwijt:	X	X	X	X
We danken u zeer voor uw medewerking aan dit onderzoek. Als u de vragenlijst hebt afgerond kunt u deze opslaan in de met u gedeelde map, of eventueel binnen uw eigen gedeelde omgeving. We verzoeken u vriendelijk ons te laten weten wanneer de vragenlijst definitief af is, hiervoor kunt u contact opnemen met uw contactpersoon zoals genoemd in het begin van deze vragenlijst.					

Oberon

Postbus 1423, 3500 BK Utrecht
t 030 230 60 90
info@oberon.eu | www.oberon.eu

Utrecht, 11 juni 2024
In opdracht van het ministerie van OCW