Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek

Sectorbeeld hogescholen

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 Kennisveiligheidsbeleid **13**
2.1 Afbakening kennisveiligheid 13
2.2 Ontwikkeling van kennisveiligheidsbeleid 14

3 Risicoanalyses **16**
3.1 Risicoanalyse 2022 16
3.2 Risicoanalyse als onderdeel van het kennisveiligheidsbeleid van hogescholen 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 23
4.3 Dilemma's en aandachtspunten 25
4.4 Lessons learned 25

5 Internationale partnerschappen en juridische kaders **26**
5.1 Internationale partnerschappen 26
5.2 Juridische kaders en gedragscodes 29
5.3 Dilemma's en aandachtspunten 31
5.4 Lessons learned 31

6 Personeelsbeleid **32**
6.1 Vertaling kennisveiligheid in personeelsbeleid 32
6.2 Dilemma's en aandachtspunten 34
6.3 Lessons learned 35

7 Conclusie en aandachtspunten **36**
7.1 Conclusie: beleid in ontwikkeling, maar niet overal relevant 36
7.2 Dilemma's 37
7.3 Aandachtpunten 38

Bijlage 1 Vragenlijst **39**

Samenvatting

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

Achtergrond, doel en aanpak
Dit sectorbeeld brengt in kaart waar hogescholen medio 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 (hierna: de Leidraad) is vertaald in instellingsbeleid en de manier waarop hogescholen 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 uitgevoerd middels een begeleide zelfevaluatie onder alle publiek bekostigde hogescholen, aangevuld met een kwalitatieve verdieping bij drie hogescholen. Hieronder vatten we de stand van zaken samen aan de hand van de hoofdstukken uit de Leidraad.

Afbakening kennisveiligheidsbeleid
De Leidraad definieert kennisveiligheid als volgt: “Met kennisveiligheid wordt 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.” 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 meerderheid van de hogescholen hanteert dezelfde definitie voor hun kennisveiligheidsbeleid. Een andere definitie die door drie hogescholen wordt gehanteerd is van het Platform Integrale Veiligheid Hoger Onderwijs, waar de nadruk ligt op bescherming van het intellectuele eigendom. Twee hogescholen vertrekken vanuit cyberveiligheid en hanteren vooralsnog die afbakening van het beleidsthema.

Het kennisveiligheidsbeleid is in de praktijk voornamelijk gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie. Er is beperkter aandacht voor het signaleren van en acteren op heimelijke beïnvloeding en ethische kwesties.

Beleid in ontwikkeling, maar niet overal relevant
Het belang van het thema kennisveiligheid wordt door hogescholen verschillend ervaren. De grotere brede hogescholen erkennen het belang van kennisveiligheid en hebben beleid ontwikkeld of zijn dat aan het doen. Van de hogescholen die de risicoanalyse in 2022 op verzoek van de minister hebben uitgevoerd was dit voor het overgrote deel hun eerste ervaring met activiteiten gericht op kennisveiligheid. Een aantal hogescholen heeft in de analyse nieuwe risico’s geïdentificeerd en daarna

[1] Sectorbeeld kennisveiligheid universiteiten 2023 | Rapport | Rijksoverheid.nl

ook concrete maatregelen getroffen. Deze hogescholen zijn sindsdien actief bezig om de adviezen van de Leidraad vorm te geven.
Een aantal andere hogescholen voert bewust geen kennisveiligheidsbeleid. Dit zijn veelal kleinere mono-sectorale hogescholen. Zij vinden het niet relevant om kennisveiligheidsbeleid te ontwikkelen, omdat zij geen sensitief onderzoek doen, geen internationale partnerschappen hebben, of nauwelijks buitenlandse werknemers en studenten hebben.

De hogescholen hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel S.1). Hier komt terug dat een deel van de hogescholen geen kennisveiligheidsbeleid ontwikkelt op onderdelen; bij de andere hogescholen is het kennisveiligheidsbeleid grotendeels nog in ontwikkeling. Daarnaast 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.
- De aspecten juridische kaders en personeelsbeleid ontbreken relatief vaker dan de andere onderdelen in het kennisveiligheidsbeleid van hogescholen.
- Kennisveiligheid wordt door een aantal hogescholen gezien als onderdeel van algemeen risicomanagement, integrale veiligheid of cyberveiligheid. Zij geven daarom aan op die onderdelen wel vaststaand instellingsbreed beleid (en dus een hoge score in de rubric) te hebben, dat echter niet specifiek is toegespitst op *kennis*veiligheid.

Tabel S.1 Fase van ontwikkeling kennisveiligheidsbeleid hogescholen, naar onderdeel Leidraad (n=37).

	Geen beleid	Gedeelten van beleid in ontwikkeling	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 verbetercyclus aanwezig	Er is een instellingsbreed risico- en beheersprogramma
Risicoanalyse	10		17		4		2	2
Risicomanagement	9		17	1	4		1	2
Fysieke en digitale beschermingsmaatregelen	8	1	13	2	9	1	1	1
Internationale partnerschappen	9		18		5	1	1	1
Juridische kaders	18		15		1			1
Personeelsbeleid	15		9	1	5	1	2	2

Risicoanalyses
De minister van OCW heeft in 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren. Ruim twee derde (26 van de 37) van de hogescholen heeft hierop een risicoanalyse uitgevoerd. Voor 22 van deze hogescholen was dit de eerste keer dat ze een risicoanalyse op kennisveiligheid uitvoerden. Acht hogescholen geven aan dat op basis van de inhoudelijke focus van het onderzoek dat binnen hun instelling plaatsvindt een risicoanalyse niet aan de orde is. Acht hogescholen hebben op basis van de risicoanalyse nieuwe risico's geïdentificeerd. Dat er bij veel hogescholen geen nieuwe risico's zijn geïdentificeerd, zegt niet dat de risicoanalyse geen effect heeft gehad: enkele hogescholen rapporteren dat de risicoanalyse heeft geleid tot meer bewustwording, en tien hogescholen geven aan dat het uitvoeren van de risicoanalyse heeft geleid tot

nieuwe (voorgenomen) maatregelen. Ook geven enkele hogescholen aan dat het thema kennisveiligheid nu is ingebed in overkoepelende risicoanalyses die periodiek door de instelling worden uitgevoerd.

Risicomanagement en fysieke en digitale maatregelen
Dertig van de 37 hogescholen hebben een bestuurlijk portefeuillehouder kennisveiligheid. Minder dan de helft van de hogescholen (15 van de 37) heeft op centraal niveau een Adviesteam Kennisveiligheid aangesteld, bij drie hogescholen is een soortgelijk team nog in oprichting.

Een essentieel onderdeel van de organisatie van kennisveiligheidsbeleid is het vergroten van het kennisveiligheidsbewustzijn onder het personeel. Docenten en onderzoekers als inhoudelijk experts zijn noodzakelijk voor het signaleren van kennisveiligheidsrisico's en worden meegenomen in het risicomanagement. Een deel van de hogescholen (9 van de 37) geeft aan bewustwordingscampagnes te voeren rondom kennisveiligheid, bijvoorbeeld door middel van al bestaande trainingen over integrale veiligheid, op strategiedagen en via presentaties. Bewustwordingscampagnes zijn vaak eerst gericht op bestuurders en lectoren, in latere fases worden andere (docent)onderzoekers en ondersteunend personeel betrokken. Een paar hogescholen houden individuele gesprekken met lectoren voor wie kennisveiligheid van groter belang is. Het overgrote deel van de hogescholen (25 van de 37) geeft aan dat binnen hun instelling nog geen specifiek beleid is om HR-medewerkers kennisveiligheidsbewust te maken, om hen in staat stellen om kennisveiligheidsrisico's te signaleren. Een aantal hogescholen geeft aan zulke campagnes momenteel te ontwikkelen.

Meer dan de helft van de hogescholen (20 van de 37) heeft een restrictief toegangsbeleid voor bepaalde ruimtes (zoals afdelingen, gebouwen of labs). Drie hogescholen geven aan dat dit beleid in ontwikkeling is, de overige veertien hogescholen geven aan geen beleid te hebben of dat dit beleid niet van toepassing is. Ook geeft het merendeel van de hogescholen (22 van de 37) aan dat ze beleid hebben omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten; dit is meer gefocust op omgang met gevoelige persoonsgegevens dan op kennisveiligheidsrisico's.

Internationale partnerschappen en juridische kaders
Twaalf hogescholen hebben momenteel een overzicht van internationale partnerschappen. Dit centrale overzicht bestaat dan voornamelijk uit overeenkomsten rondom onderwijs, zoals studentuitwisselingen. Overzichten van onderzoekspartnerschappen zijn in mindere mate aanwezig. Veel hogescholen vinden een dergelijk centraal overzicht niet van toepassing, omdat zij geen internationale partnerschappen hebben waarbij samengewerkt wordt op kennisveiligheidsgevoelige thema's.
Veel hogescholen geven aan geen ervaring te hebben met *due diligence* voor het aangaan van internationale partnerschappen en processen hiervoor niet nodig te vinden, omdat ze weinig tot geen kennisveiligheidsgevoelig onderzoek doen. Bij de hogescholen die wel bezig zijn met een partneracceptatiebeleid, is dat ingebed in bestaande afdelingen en teams, zoals de inkoopafdeling, de afdeling juridische zaken of de *international office*.
Hogescholen geven in grote mate aan dat dual-use-technologie niet wordt onderzocht of ontwikkeld aan hun instelling, waardoor beleid of compliance met die juridische kaders niet relevant is.

Personeelsbeleid
De meerderheid van de hogescholen (22 uit 37) ontwikkelt of heeft al aandacht voor kennisveiligheid als onderdeel van het personeelsbeleid. Negen van de 37 hogescholen geven aan in meer of mindere mate veiligheidsrisico's mee te wegen bij de werving en selectie van nieuwe medewerkers. Zij volgen formele of informele procedures en richtlijnen, of controleren (een deel) van het nieuwe personeel op mogelijke

kennisveiligheidsrisico's middels het toetsen van zijn of haar achtergrond. Deze hogescholen vragen veelal om een Verklaring Omtrent het Gedrag (VOG), en vullen dit aan met een referentiecheck, een check op getuigschriften of een achtergrondscreening.
Tweederde van de hogescholen (24 van de 37) heeft geen specifiek beleid om te voorkomen dat de sociale veiligheid wordt aangetast door (heimelijke) beïnvloeding. Een aantal van hen geeft expliciet aan dat er in de risicoanalyse geen risico's op heimelijke beïnvloeding zijn gesignaleerd of dat zij geen medewerkers uit risicolanden in dienst hebben.

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

- Het kennisveiligheidsbeleid is in de praktijk vooral 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 hogescholen die in de regel geen nieuwe technologie ontwikkelen of fundamenteel onderzoek doen. Hogescholen vragen zich af hoe sensitief toegepaste kennis kan zijn, en hoe proportioneel diverse beheersmaatregelen daarvoor zijn.
- 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 hogescholen moet worden meegewogen. Hogescholen werken in hun praktijkgericht onderzoek samen met bedrijven die wellicht actief zijn op sensitieve kennisgebieden. Ook lopen studenten stages bij bedrijven en instituten waar kennisveiligheid een belangrijke overweging kan zijn. Hoewel die stagebedrijven en instituten in principe zelf verantwoordelijk zijn voor hun eigen kennisveiligheidsbeleid, geven enkele hogescholen aan dat ook zij verantwoordelijkheid dragen als **toegangspoort tot hun (regionale) netwerk**. Hogescholen vragen zich af hoe zij hun positie in het netwerk met bedrijven en instituten mee kunnen nemen in hun risicoanalyses.
- Een aantal hogescholen is nog zoekende in de **samenwerking tussen de centrale en decentrale niveaus**. Het bestuur zoekt naar een balans tussen het creëren van bewustzijn en analyseren van potentiële risico's bij *alle* afdelingen, wat kan leiden tot paranoia, discriminatie of irritatie, en beleid gericht op *specifieke* afdelingen, waardoor bepaalde medewerkers of afdelingen wellicht onvoldoende bewust raken van kennisveiligheid.

Aandachtpunten
Uit het sectorbeeld komen ook een aantal aandachtspunten voor het landelijk beleid:

- **Expertise voor het signaleren van kennisveiligheidsrisico's**. Een groot aantal hogescholen ontwikkelt geen kennisveiligheidsbeleid omdat zij aangeven dat er op hun instelling geen kennisveiligheidsrisico's spelen. Een risico hierbij is dat met onvoldoende ontwikkelde expertise het ook niet goed mogelijk is om kennisveiligheidsrisico's te signaleren. Een aandachtspunt is dus dat hogescholen goed in staat dienen te worden gesteld om kennisveiligheidsrisico's te detecteren, zonder een disproportioneel apparaat te ontwikkelen voor kennisveiligheidsbeleid voor de omgang met eventuele kennisveiligheidsrisico's.
- **Samenwerking tussen hogescholen**. Er zijn kansen voor (intensiever) samenwerking tussen hogescholen onderling en met universiteiten. Zeker waar het niet proportioneel is voor elke hogeschool om expertise te ontwikkelen, kan het nuttig zijn om in sterkere mate samen te werken.

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 hogescholen. Eerder dit jaar is een sectorbeeld voor de universiteiten verschenen,[2] later volgt nog een sectorbeeld voor de KNAW- en NWO-instituten.

1.1 Achtergrond van het onderzoek

Op 31 januari 2022 hebben de Nederlandse kennissector en de Rijksoverheid gezamenlijk de Nationale Leidraad Kennisveiligheid (hierna: de Leidraad) gepubliceerd,[3] 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.

In het bestuursakkoord 2022 hoger onderwijs en wetenschap is afgesproken dat een externe audit zal plaatsvinden op de (mate van) implementatie van de Leidraad.[4] In het spoeddebat kennisveiligheid was deze externe audit eerder toegezegd aan de Tweede Kamer.[5] 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.

Omdat kennisveiligheid een thema is dat de laatste twee jaar aan urgentie heeft gewonnen en nog volop in ontwikkeling is, is er geen normenkader voor een inhoudelijke audit. Het Wetsvoorstel Screening Kennisveiligheid,[6] waarin moet worden uitgewerkt welke kennisgebieden als sensitief worden aangemerkt, is bijvoorbeeld nog in ontwikkeling (en het staat ook nog niet vast of dit wetsvoorstel voldoende basis geeft voor een inhoudelijke audit.) Daarom volgt dit onderzoek de lijn van een procesevaluatie.

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[7] van kennisveiligheid uit te voeren of te actualiseren. 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, zodat komende jaren de ontwikkeling van het kennisveiligheidsbeleid op sectorniveau in kaart kan worden gebracht.

---

2 Sectorbeeld kennisveiligheid universiteiten 2023 | Rapport | Rijksoverheid.nl

3 Deze is opgesteld door UNL, KNAW, de VH, NFU, de TO2 federatie, NWO en OCW. Zie: Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken | Rapport | Rijksoverheid.nl

4 Bestuursakkoord 2022 hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl

5 Commissiedebat Hoger Onderwijs- Onderzoek- en Wetenschapsbeleid (23 juni 2022). *Spoeddebat kennisveiligheid.*

6 Kamerbrief inzake tijdpad wetstraject Screening Kennisveiligheid en uitwerking amendement middelen kennisveiligheidsbeleid | Kamerstuk | Rijksoverheid.nl

7 Zie: Afschrift brief aan kennisinstellingen Nationale Leidraad Kennisveiligheid | Brief | Rijksoverheid.nl

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 hogescholen. We beschrijven de resultaten zo dat dit rapport zelfstandig leesbaar is zonder benodigde voorkennis van andere rapporten; om deze reden zijn beschrijvingen uit het sectorbeeld universiteiten herhaald. In dit rapport wordt de wijze waarop en de mate waarin de Leidraad is vertaald in het instellingsbeleid en de manier waarop risicoanalyses op internationale samenwerkingen zijn uitgevoerd in beeld gebracht. Dit leidt tot de volgende centrale onderzoeksvraag: *Waar staan de hogescholen 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**.[8] 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 hogescholen zich geconfronteerd zien en eventuele *lessons learned* waar zij van elkaar kunnen leren. Naast dit sectorbeeld ontvangen alle hogescholen daarom een individuele terugkoppeling in de vorm van een instellingsbeeld waarin hun antwoorden worden gecontextualiseerd binnen het sectorbeeld.

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 instellingen. De begeleiding bestond eruit dat hogescholen een vragenlijst voorgelegd kregen die zij puntsgewijs dienden te beantwoorden. In het geval een vraag niet goed begrepen werd konden hogescholen contact opnemen met de onderzoekers.

1.3.1 Voorbereiding

De voorbereidingsfase liep gelijk op met die van de universiteiten en begon met een startgesprek over de onderzoeksopzet met het ministerie van OCW. Direct daarna zijn we gestart met het uitwerken van de concept-vragenlijst aan de hand van de Leidraad. Door de kwalitatieve aard van de vragenlijst bestaat deze voor een groot gedeelte uit open vragen. Om meer inzichten op te halen voor de ontwikkeling van de vragenlijst, hebben we verkennende interviews gehouden met vertegenwoordigers van het Loket Kennisveiligheid, de UNL en de VH. De concept-vragenlijst is vervolgens ter toetsing voorgelegd aan een twee universiteiten en een hogeschool. Zij hebben in gesprek met een onderzoeker de vragenlijst doorgelopen en van commentaar voorzien. Omdat de vragenlijst was gebaseerd op de gezamenlijke Leidraad, was voor de hogescholen alleen een tekstuele aanpassing van de vragenlijst nodig.
De vragenlijst is vervolgens besproken met de **klankbordgroep** die voor dit onderzoek is ingesteld. Het ministerie van OCW heeft ten slotte de vragenlijst besproken met de **Regiegroep** Kennisveiligheid (het bestuurlijk overleg met vertegenwoordiging vanuit VH, UNL, KNAW, NWO en NFU). De vragenlijst zoals die is gehanteerd voor de hogescholen is opgenomen in bijlage 1.

[8] AWTI (2022). Kennis in conflict. Veiligheid en vrijheid in balans.

Tabel 1.1 Onderzoeksopzet hogescholen in vogelvlucht

Fase	Activiteiten	Periode
Voorbereiding	• Startgesprek • Literatuuronderzoek • Verkennende interviews (3) • Opzet vragenlijst zelfevaluatie • Toetsen vragenlijst bij instellingen (3) • Bespreking vragenlijst met klankbordgroep • Bespreking vragenlijst met de Regiegroep Kennisveiligheid	December 2022 tot en februari 2023 (voor wo en hbo)
Uitvoering zelfevaluatie door de instellingen	• Uitzetten vragenlijst en persoonlijk contact • Invullen vragenlijst door instellingen • Nazorggesprek en duiding	Mei en juni
Kwalitatieve verdieping	• Selectie en benadering cases • Uitvoering en verslaglegging cases (3)	Juli Augustus t/m oktober
Analyse en rapportage	• Analyse vragenlijsten • Rapportage • Bespreken conceptrapport met klankbordgroep	September September en oktober November 2023

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, KNAW, twee universiteiten en twee UMC's. Voor de bespreking van het concept sectorbeeld hogescholen is de klankbordgroep uitgebreid met vertegenwoordigers vanuit twee hogescholen.

1.3.2 Uitvoering zelfevaluatie

De goedgekeurde vragenlijst voor de zelfevaluatie voor het sectorbeeld hogescholen is eind april 2023 uitgezet onder contactpersonen van alle (37) publiek bekostigde hogescholen[9] via een beveiligde omgeving. Deze is vervolgens door hen in samenspraak met andere relevante personen binnen de instelling ingevuld. Met de contactpersonen hielden we ook direct contact over de voortgang, eventuele vragen en tijdige oplevering.

1.3.3 Aanvullend kwalitatief verdiepend onderzoek

Na de analyse van de vragenlijsten volgde een kwalitatief, verdiepend casestudy onderzoek bij drie hogescholen. 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. Het gaat hierbij dus om een verdiepend inzicht in mechanismes en fenomenen (in dit geval: beleidsprocessen en uitdagingen), niet om een representatief beeld van instellingen die vooroplopen of juist nog meer in de ontwikkelingsfase zitten. Bij de selectie hebben we gezocht naar een spreiding over:

[9] In totaal hebben 37 hogescholen meegedaan aan de zelfevaluatie, dit zijn de 36 hogescholen en het Nederlands Instituut Publieke Veiligheid (NIPV), een kennisinstituut dat ook opleidingen aanbiedt en onderzoek doet middels lectoraten.

- achtergrondkenmerken (twee brede hogescholen en een monosectorale hogeschool); 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 klankbordgroep. Vanwege anonimiteit van de deelnemende instellingen, is de daadwerkelijke selectie gedaan door het onderzoeksteam en *niet* gecommuniceerd met de klankbordgroep of het ministerie van OCW. Voor elke case voerden we gesprekken met betrokkenen op meerdere niveaus binnen de instelling. Hierbij onderscheiden we het centrale niveau (waaronder de bestuurlijk portefeuillehouder, het adviesteam en eventueel anderen), het decentrale niveau van bijvoorbeeld instituutsdirecteuren, lectoren en HR-verantwoordelijken. In totaal zijn 17 gesprekken gevoerd op de drie instellingen gezamenlijk.

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 integraal samengebracht in dit sectorbeeld voor de hogescholen.

2 Kennisveiligheidsbeleid

In dit hoofdstuk gaan we eerst in algemene zin in op het kennisveiligheidsbeleid van hogescholen. In paragraaf 2.1 beginnen we met de afbakening van het beleidsthema kennisveiligheid. In paragraaf 2.2 beschrijven we het proces van beleidsontwikkeling aan hogescholen.

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.[10] In dit rapport schrijven we in het kort over **sensitieve kennis en technologie**, **heimelijke beïnvloeding** en **ethische kwesties** als de onderwerpen van kennisveiligheid.

Het hbo kent een grote diversiteit aan instellingen. De kleinste hogeschool heeft 540 (pabo) studenten, de grootste 45 duizend studenten. Er zijn er 11 monosectorale hogescholen met minder dan 2.000 studenten, maar ook 12 hogescholen met meer dan 20 duizend studenten. Bijna alle studenten volgen een hbo-bacheloropleiding; 15 duizend van de half miljoen hbo-studenten volgen een masteropleiding. Per instelling varieert dat van 7 tot 2.500 studenten.[11]
Onderwijs is de kernfunctie van hogescholen. Het praktijkgericht onderzoek aan hogescholen is de afgelopen jaren wel gegroeid, maar hogescholen besteedden in 2019 6% van hun middelen aan onderzoek. Het hbo kent ongeveer 700 lectoren, bij de lectoraten werken men in 2020 ongeveer 2.700 fte aan personeel op 40 duizend fte aan personeelsleden voor het hele hbo.[12]
Een deel van de hbo-opleidingen heeft een sterk internationaal karakter. Zo is in de agro & food sector een buitenlandstage gemeengoed en kennen opleidingen in de kunstsector, *hospitality management* en *international business* een relatief grote instroom aan buitenlandse studenten. Andere opleidingen hebben een sterk nationale of regionale focus. Lerarenopleidingen kennen bijvoorbeeld bijna geen internationale studenten en een beperkte uitgaande studiepuntmobiliteit.[13] Van de ongeveer half miljoen hbo-studenten zijn in het jaar 2022-2023 bijna 37 duizend internationale studenten, waaronder ongeveer 9,5 duizend studenten van buiten de EER.[14]

---

10 kamerbrief over maatregelen kennisveiligheid hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl

11 Gegevens over 2022, zie Feiten en Cijfers Vereniging Hogescholen

12 Zie Praktijkgericht onderzoek hogescholen | Rathenau Instituut en Dashboard Personeel Vereniging Hogescholen

13 VH en VSNU (2018) Internationaliseringsagenda Hoger Onderwijs

14 Nuffic (2023). Incoming degree mobility in Dutch higher education 2022-23

De meerderheid van de hogescholen hanteert de definitie van de Leidraad voor hun kennisveiligheidsbeleid. In hun beantwoording gebruiken 22 hogescholen dezelfde definitie, waarbij negen hogescholen expliciet verwijzen naar de Leidraad en drie hogescholen verwijzen naar het ministerie of Loket Kennisveiligheid. Een andere definitie die door drie hogescholen wordt gehanteerd is van het Platform Integrale Veiligheid Hoger Onderwijs.[15] In deze definitie ligt de nadruk op het intellectuele eigendom, ook wordt heimelijke beïnvloeding genoemd:

> Kennisveiligheid betreft de veiligheid van het intellectuele eigendom van hogescholen of universiteiten, zoals wetenschappelijke kennis, onderzoeksresultaten en innovaties. Ook het tegengaan van ongewenste beïnvloeding en dual-use gebruik van kennis valt onder dit thema. Voorbeelden van dreigingen zijn (digitale) spionage, diefstal van gegevens en het verlenen van gunsten in ruil voor tegenprestaties.

Twee hogescholen vertrekken vanuit cyberveiligheid en hanteren vooralsnog die afbakening van het beleidsthema. Twee hogescholen noemen alleen ongewenste overdracht van sensitieve kennis en technologie, één hogeschool vult hier ook nog heimelijke beïnvloeding op aan. Eén hogeschool definieert kennisveiligheid als de algehele integriteit en veiligheid van studenten en medewerkers. Ten slotte geven vier hogescholen aan geen (formele) definitie te hanteren.

2.2 Ontwikkeling van kennisveiligheidsbeleid

In 2022 is (de aandacht voor) het kennisveiligheidsbeleid van hogescholen in een stroomversnelling geraakt. Bij twintig hogescholen wordt 2022 aangegeven als de start van het kennisveiligheidsbeleid, waarbij zeven hogescholen aangeven dat de oproep van de minister voor een risicoanalyse de aanleiding hiertoe vormde (zie hoofdstuk 3). Zes hogescholen startten tussen 2019 en 2021 met kennisveiligheidsbeleid; twee hiervan naar aanleiding van de ontwikkeling van de Leidraad, die in januari 2022 is gepubliceerd. Drie hogescholen geven aan dat zij in 2023 zijn gestart met de ontwikkeling. Ten slotte geven vijf hogescholen aan geen beleid te hebben; één hiervan heeft wel de ambitie voor beleidsontwikkeling en één geeft wel aan een richtlijn te hanteren voor het aangaan van internationale partnerschappen.
Een drietal hogescholen geeft in aanvulling aan dat zij al langer bezig zijn met cyberveiligheidbeleid, waarmee een basis is gelegd voor kennisveiligheidsbeleid.

De ontwikkeling van het kennisveiligheidsbeleid is in sterke mate afhankelijk van de uitgevoerde risicoanalyse (zie hoofdstuk 3). Twaalf hogescholen geven aan geen verder kennisveiligheidsbeleid te ontwikkelen, omdat er geen sprake is van risico's die daarom vragen. Zes hogescholen onderzoeken nog hun behoefte aan verder kennisveiligheidsbeleid. 17 hogescholen hebben de intentie om het kennisveiligheidsbeleid verder te ontwikkelen, zij noemen onder meer plannen om de Leidraad verder te implementeren, personeel aan te nemen of kennisveiligheidsplannen op te stellen en tot uitvoering te brengen. Bij twee hogescholen wordt de komende tijd primair ingezet op het vergroten van het bewustzijn.

De hogescholen hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel 2.1).[16] Daarbij zien we een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad:

---

15 Kennisveiligheid - Platform Integrale Veiligheid Hoger Onderwijs (integraalveilig-ho.nl)

16 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.

- 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.
- De aspecten juridische kaders en personeelsbeleid ontbreken relatief vaker dan de andere onderdelen in het kennisveiligheidsbeleid van hogescholen.
- Kennisveiligheid wordt door een aantal hogescholen gezien als onderdeel van algemeen risicomanagement, integrale veiligheid of cyberveiligheid. Zij geven daarom aan op die onderdelen wel vaststaand instellingsbreed beleid (en dus een hoge score in de rubric) te hebben, dat echter niet specifiek is toegespitst op *kennis*veiligheid.

Dit laatste punt bemoeilijkt interpretatie van de tabel. Het is immers mogelijk dat de ene hogeschool aangeeft dat zij geen toegespitst kennisveiligheidsbeleid voert ('geen beleid'), terwijl een andere hogeschool met vergelijkbaar beleid aangeeft dat dit wordt gedekt door het beleid op integrale veiligheid ('er is een instellingsbreed risico- en beheersprogramma').

Tabel 2.1. Zelfscores op fase van beleidsontwikkeling. (verschillende hogescholen hebben op één of meer onderdelen geen score ingevuld. Hierdoor is de n per onderwerp minder dan 37)

	Geen beleid	Gedeelten van beleid in ontwikkeling	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 verbetercyclus aanwezig	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Risicoanalyse	10		17		4		2	2
Risicomanagement	9		17	1	4		1	2
Fysieke en digitale beschermings-maatregelen	8	1	13	2	9	1	1	1
Internationale partnerschappen	9		18		5	1	1	1
Juridische kaders	18		15		1			1
Personeelsbeleid	15		9	1	5	1	2	2

Evaluaties van het kennisveiligheidsbeleid worden beperkt toegepast. Acht hogescholen zijn voornemens om evaluaties uit te voeren, bij nog eens drie hogescholen zal dit onderdeel vormen van bredere interne evaluaties op bijv. integrale veiligheid. Een drietal hogescholen noemt hierbij de PDCA aanpak (Plan, Do, Check, Assess) als model. Bij vijf hogescholen is de evaluatie van het beleid in afwachting van de beleidsontwikkeling. Twintig hogescholen geven aan geen evaluaties van het kennisveiligheidsbeleid te zullen uitvoeren, bij gebrek aan noodzaak voor beleid (zie boven).

3 Risicoanalyses

De minister van OCW heeft op 4 april 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren.[17] 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 de instelling 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 op welke manier instellingen hieraan invulling hebben gegeven. Vervolgens gaan we in op de manier waarop hogescholen 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 instellingen 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.[18] 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 wordt de mogelijkheid aangestipt om contact op te nemen met het Loket Kennisveiligheid voor informatie en advies vanuit de Rijksoverheid. De minister is zich er hierbij van bewust dat er grote verschillen bestaan tussen de instellingen, en geeft 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 hogescholen

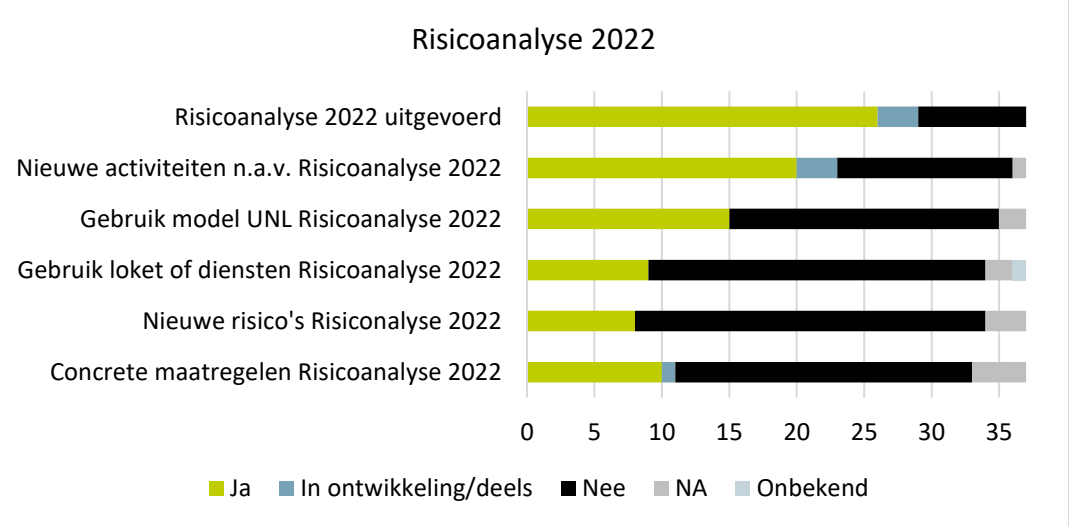
Ruim twee derde (26 van de 37) van de hogescholen heeft naar aanleiding van de oproep van de minister een risicoanalyse uitgevoerd. Drie hogescholen zijn hier op dit moment nog mee bezig. 20 hogescholen geven aan dat zij naar aanleiding van de oproep van de minister nieuwe of andere activiteiten hebben ontplooid in vergelijking met risicoanalyses die de instelling daarvoor uitvoerde. Voor een aantal hogescholen was dit de eerst keer dat ze een risicoanalyse op het gebied van

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

kennisveiligheid hebben uitgevoerd, voor anderen was dit een aanleiding om dat structureel uit te gaan voeren (zie ook paragraaf 3.2).
Acht hogescholen geven aan geen risicoanalyse te hebben uitgevoerd. Een deel van hen licht toe dat dit te maken heeft met de inhoudelijke focus van het onderwijs en onderzoek dat binnen de instelling plaatsvindt (vijf van deze acht zijn hogescholen die zich richten op kunsten of het opleiden van leraren). Als er geen risico's zijn, is het niet mogelijk om een (gestructureerde) risicoanalyse uit te voeren. Sommige instellingen rapporteren dat het kennisveiligheidsbeleid op de betreffende hogeschool nog in de kinderschoenen staat en dat zij hier nog mee moeten starten na juni 2023.

Er bestaan verschillende modellen aan de hand waarvan risicoanalyses kunnen worden uitgevoerd. 15 hogescholen hebben gebruik gemaakt van het model Risicoanalyse 2022 van de UNL. Ook geven enkele hogescholen aan gebruik gemaakt te hebben van de Kwetsbaarheidsanalyse Spionage (KWAS) van de AIVD of van een model dat zelf is opgesteld op basis van verzamelde informatie.
Negen hogescholen hebben gebruik gemaakt van advies van het Loket Kennisveiligheid (hierna: het Loket) of van contacten bij de veiligheidsdiensten bij het uitvoeren van de risicoanalyse. Bovendien leidde de aandacht voor kennisveiligheid bij een hogeschool zelf al tot meer bewustwording en daarmee tot het voorleggen van casussen aan het Loket. Ook hebben twee hogescholen de AIVD en het Loket gevraagd om mee te denken in het vormgeven van de awareness-activiteiten, en geven twee hogescholen aan de uitkomsten van de risicoanalyse te hebben gespiegeld bij het Loket.

Figuur 3.1 Overzicht activiteiten op risicoanalyses



Acht hogescholen hebben op basis van de risicoanalyse nieuwe risico's geïdentificeerd. Er worden risico's genoemd op verschillende onderwerpen, zoals samenwerkingen, sensitieve kennis en personeelsbeleid. Dat er bij veel hogescholen geen nieuwe risico's zijn geïdentificeerd, zegt niet dat de risicoanalyse geen effect heeft gehad: enkele hogescholen rapporteren dat er door de risicoanalyse meer bewustwording is gecreëerd, en tien hogescholen geven aan dat het uitvoeren van de risicoanalyse heeft geleid tot nieuwe (voorgenomen) maatregelen. Maatregelen richten zich bijvoorbeeld op internationale relaties en dienstreizen, formalisering van risicoanalyse en -management op het gebied van kennisveiligheid en het creëren van meer bewustzijn op het gebied van kennisveiligheid binnen de eigen instelling. Er zijn ook hogescholen die geen nieuwe maatregelen hebben genomen, bijvoorbeeld omdat zij de geïdentificeerde risico's al eerder in beeld hadden.
Voor een overzicht van de antwoorden van hogescholen, zie Figuur 3.1.

3.2 Risicoanalyse als onderdeel van het kennisveiligheidsbeleid van hogescholen

Hogescholen die de risicoanalyse niet als relevant beschouwen binnen de scope van hun onderzoek, hebben de analyse óf niet uitgevoerd, of concluderen dat het niet nodig is om hier verdieping in aan te brengen in de vorm van beleid. In de verdiepende gesprekken is aangedragen dat hogescholen soms inderdaad geen risico zien voor de kennis die zij zelf in huis hebben, bijvoorbeeld omdat dit zich richt op een specifiek thema of een hoger TRL-niveau waarbij de onderliggende kennis vaak al eerder (elders) is ontwikkeld, toegepast en (dus) verspreid. Zij vinden de risicoanalyse toch relevant vanuit de toegang die zij studenten en medewerkers bieden tot het Nederlandse hoger onderwijs- en onderzoekssysteem. Een student kan bijvoorbeeld wel via zijn of haar opleiding bij een kennissensitief bedrijf of instituut gaan werken of stagelopen, en via een hbo-bachelorprogramma kan een student eenvoudiger doorstromen naar meer sensitieve vervolgstudies. Ondanks dat het risico binnen de eigen opleiding of instelling dan gering lijkt, zien sommige hogescholen dus toch de relevantie van het grondig uitvoeren van een risicoanalyse. Zo vermijden zij dat er indirect risico's, met bijbehorende (imago)schade, ontstaan voor henzelf of partners.

Bij de groep hogescholen die de risicoanalyse wel hebben uitgevoerd (26 van de 37), geven 22 hogescholen aan dat de risicoanalyse naar aanleiding van de oproep van de minister de eerste risicoanalyse was die is uitgevoerd door de instelling. Enkele hogescholen hebben naar aanleiding van de oproep de al uitgevoerde risicoanalyses binnen hun hogeschool geïntensiveerd, bijvoorbeeld door deze door te ontwikkelen van een ad hoc-uitvoering naar een structurele uitvoering, of van een gedecentraliseerd naar een gecentraliseerd niveau. Ook geven enkele hogescholen aan dat het thema nu is ingebed in overkoepelende risicoanalyses die periodiek door de instelling worden uitgevoerd. Tenslotte geeft een aantal instellingen aan specifieke focusgebieden te hebben toegevoegd aan hun analyses.

De risicoanalyses van de hogescholen 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 in kaart brengen van 'kroonjuwelen' en (d) gestandaardiseerde processen die bij een bepaald risiconiveau in werking treden. De inzichten die dit oplevert, zijn weergegeven in Tabel 3.1.

Tabel 3.1.Onderdelen risicoanalyses hogescholen

	Uitgevoerd	In ontwikkeling	Niet van toepassing
Identificatie sensitieve kennisgebieden	17	2	8
Eigen lijst sensitieve kennisgebieden	6	1	20
Identificatie kroonjuwelen	6	3	12
Standaard-processen	6	5	20

De meeste instellingen kiezen er niet voor om een eigen lijst van sensitieve kennisgebieden te hanteren of om hun 'kroonjuwelen' in kaart brengen. Kroonjuwelen zijn de gebieden waarop er risico's verbonden zijn aan kennisoverdracht en waar de instelling internationaal toonaangevend is. Ook zijn er weinig hogescholen waar standaardprocessen in werking treden bij een bepaald risiconiveau; afspraken hierover vinden veel hogescholen niet van toepassing.

3.3 Dilemma's en aandachtpunten

Hogescholen geven een viertal dilemma's en aandachtspunten mee op het gebied van risicoanalyse(s). Ten eerste vinden hogescholen tijdens de risicoanalyse het geregeld lastig om te bepalen of onderzoek op sensitieve kennisgebieden ook betekent dat er concrete risico's zijn. Dat heeft onder meer te maken met het niveau van de kennis (toepassingsgericht, hoger TRL-niveau waarbij de onderliggende kennis vaak al eerder (elders) is ontwikkeld, toegepast en (dus) verspreid). Er worden nu potentiële risicogebieden herkend, maar dan is het moeilijk om hier specifiek duiding aan te geven. Instellingen weten vaak ook niet hoe die risico's bij andere instellingen of door overheden ingeschat worden, of en hoe hiernaar gehandeld wordt en in welke mate deze relevant zijn voor hun eigen instelling.

Ten tweede, doordat hogescholen vaker dan universiteiten een specifieke focus kennen (zoals de pabo's of de kunstacademies), is het moeilijk om standaardmodellen toe te passen in de praktijk. Dit vraagt een extra afweging van hogescholen met betrekking tot welke thema's relevant zijn, en hoe die uitgevraagd kunnen worden.

Ten derde blijkt uit de verdiepende gesprekken dat hogescholen nog zoekende zijn in de samenwerking tussen de centrale en decentrale niveaus. Het centrale bestuur zoekt naar een balans tussen het creëren van bewustzijn en analyseren van potentiële risico's bij *alle* afdelingen, wat kan leiden tot paranoia, discriminatie of irritatie, en beleid gericht op *specifieke* afdelingen, waardoor bepaalde medewerkers of afdelingen wellicht onvoldoende bewust raken van kennisveiligheid. Ook schatten medewerkers op centraal en decentraal niveau risico's anders in.

Ten slotte zoeken hogescholen – zeker voor afdelingen waar het risico lager wordt ingeschat –naar de balans tussen administratieve lasten en het uitvoeren van een grondige risicoanalyse als onderdeel van het kennisveiligheidsbeleid.

3.4 Lessons learned

Er komen beperkt geleerde lessen naar voren uit de vragenlijst met betrekking tot de risicoanalyse, we destilleren er twee. Ten eerste is het bewustzijn van hogescholen van risico's met betrekking tot kennisveiligheid bij meerdere instellingen aangewakkerd of toegenomen door de (oproep voor) de risicoanalyse. Daarnaast is beleid op het gebied van kennisveiligheid nog vaak decentraal en ad hoc ingericht. Het wordt steeds meer geformaliseerd, en een aantal hogescholen is bezig met het ontwikkelen van standaardprocedures, aanspreekpunten en bewustzijn binnen de instelling.

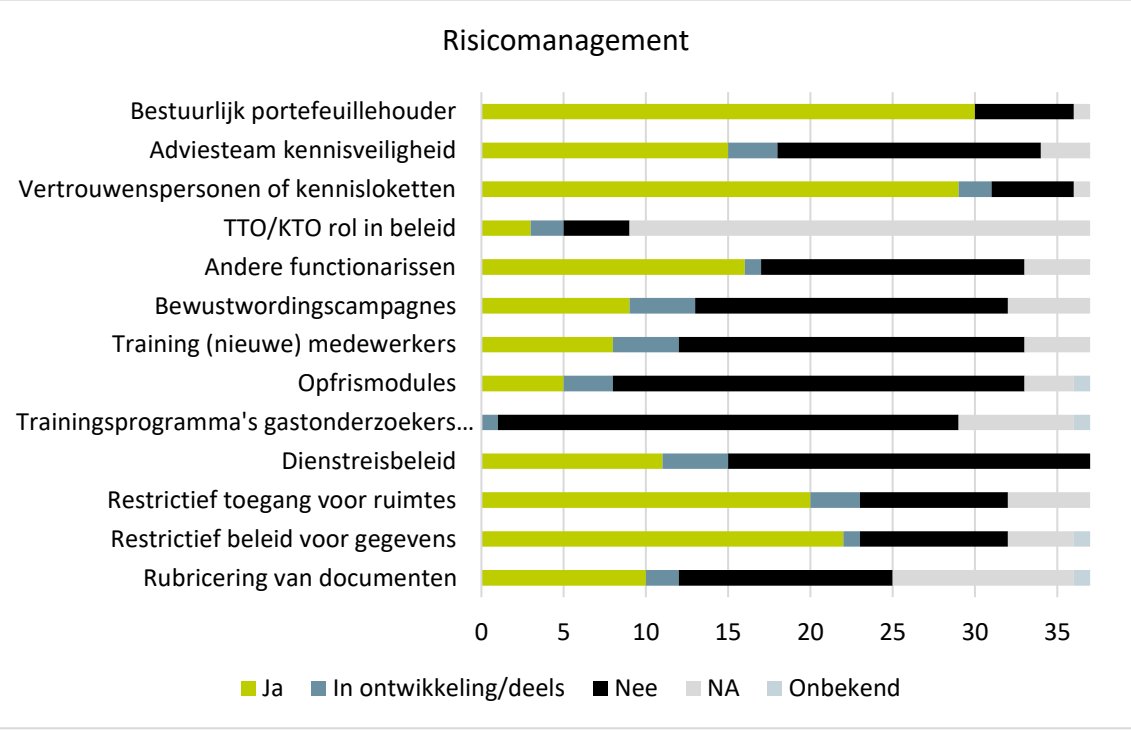
4 Risicomanagement en fysieke en digitale maatregelen

In dit hoofdstuk beschrijven we hoe hogescholen 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. De hogescholen zijn zeer divers in de mate van centralisatie: kleine hogescholen hebben veelal een centrale organisatie, terwijl grotere hogescholen vaker meer decentraal zijn georganiseerd. Hoe de afstemming wordt verkregen tussen deze verschillende lagen staat centraal in paragraaf 4.1. Daarna gaan we in op het toegangsbeleid tot ruimtes en digitale gegevens als onderdeel van risicomanagement in paragraaf 4.2. In paragraaf 4.3 bespreken we de dilemma's en uitdagingen specifiek op dit onderdeel van het kennisveiligheidsbeleid, gevolgd door *best practices* en *lessons learned* in paragraaf 4.4.

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. Figuur 4.1 geeft een overzicht van de activiteiten van hogescholen op het gebied van risicomanagement.

Figuur 4.1 Overzicht activiteiten risicomanagement



Het beleid voor risicomanagement van kennisveiligheid heeft op een deel van de hogescholen de aandacht (zie eerder Tabel 2.1). Vijf hogescholen geven aan beleid omtrent risicomanagement van kennisveiligheid te hebben wat (deels) is vastgesteld en waarvan de uitvoering aantoonbaar is. Twee hogescholen geven aan dat er voor dit beleid al een verbetercyclus aanwezig is. Achttien hogescholen geven aan dat dit beleid nu in ontwikkeling is, tien hogescholen geven aan geen beleid te hebben. Van twee hogescholen is de stand van hun beleid voor risicomanagement onbekend.

Dertig hogescholen hebben een **bestuurlijk portefeuillehouder** kennisveiligheid aangewezen. In de verdiepende gesprekken wordt aangegeven dat een lid van het CvB als bestuurlijk portefeuillehouder kennisveiligheid incidenteel betrokken wordt bij casussen en op de hoogte blijft van landelijk/internationaal beleid en ideeën omtrent kennisveiligheid. De meeste hogescholen hebben geen verdere informatie gegeven over hoe deze rol precies wordt ingevuld of over het niveau van betrokkenheid van de portefeuillehouder in het domein kennisveiligheid.

4.1.1 Organisatieonderdelen betrokken bij kennisveiligheid

Minder dan de helft van de hogescholen (15 van de 37) heeft op centraal niveau een **adviesteam Kennisveiligheid** aangesteld. Enkele hogescholen (drie van de 37) geven aan dat een soortgelijk team nog in oprichting is. 19 hogescholen geven aan geen soortgelijk team te hebben, waarvan drie hogescholen toelichten een adviesteam kennisveiligheid op centraal niveau voor hun instelling niet van toepassing is.

Het adviesteam bestaat, waar aanwezig, veelal uit een kleine kern (tot 6 à 7 leden) met daaromheen een schil van experts en adviseurs die op ad hoc basis beschikbaar zijn voor specifieke casussen. De exacte samenstelling van het adviesteam varieert tussen hogescholen. Het kernteam bestaat vaak uit een programmamanager/themahouder Kennisveiligheid (indien aanwezig), coördinator Integrale Veiligheid, de Chief Information Security Officer (CISO) en overige beleidsmedewerkers. In een aantal gevallen zitten er ook medewerkers met kennis van juridische zaken, HR, export control en internationale samenwerkingen in het kernteam of zijn deze medewerkers deel van de bredere schil rondom het adviesteam. De positionering van het adviesteam verschilt tussen hogescholen. Bij diverse hogescholen is kennisveiligheid ondergebracht bij een programma of de afdeling integrale veiligheid, bij sommige hogescholen is dit een apart team met een specifiek mandaat.

Het adviesteam is primair verantwoordelijk voor de ontwikkeling van het kennisveiligheidsbeleid en is veelal het aanspreekpunt voor kennisveiligheidsvraagstukken vanuit decentrale onderdelen als instituten, centres of experise, kenniscentra, academies of faculteiten. Het adviesteam kan ook dienen als loket voor ondersteunende afdelingen voor vragen over onder andere personeelsbeleid en internationale partnerschappen. Een aantal hogescholen geeft aan dat wanneer het adviesteam de vraag niet zelfstandig kan beantwoorden, zij de vraag voorlegt bij het Loket Kennisveiligheid.

Het verkrijgen van beleidsmatige afstemming tussen het instellingsbrede en decentrale kennisveiligheidsbeleid is bij de meeste hogescholen belegd in bestaande overleggen. Een deel van de hogescholen geeft aan dat de manier waarop beleidsmatige afstemming wordt geregeld nog in ontwikkeling is. Een aantal hogescholen geeft ook aan door hun beperkte omvang weinig afstand te ervaren tussen centraal en decentraal, waardoor afstemming niet geformaliseerd hoeft te worden. Dit beeld wordt ook bevestigd in de verdiepende gesprekken. In verdiepende gesprekken geeft een hogeschool aan dat hun decentrale organisatie het verkrijgen van beleidsmatige afstemming bemoeilijkt.

Bij het merendeel van hogescholen 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 onder andere ook voor vragen over wetenschappelijke integriteit, databeveiliging, privacy vraagstukken en ongewenst gedrag. Dit betekent dus ook dat hogescholen die op deze vraag 'nee' hebben geantwoord niet noodzakelijkerwijs helemaal

geen vertrouwenspersonen hebben, maar hoogstens dat hun vertrouwenspersonen niet te benaderen zijn voor kennisveiligheidsvraagstukken.

De meeste hogescholen beschikken niet over **technology/knowledge transfer offices (TTO/KTO)**, die verantwoordelijk zijn voor toepassing en valorisatie van kennis. Hogescholen die wel een TTO of KTO hebben, nemen deze beperkt mee in hun kennisveiligheidsbeleid. Ze zijn over het algemeen geen onderdeel van de ontwikkeling van het kennisveiligheidsbeleid; in een aantal gevallen worden ze wel op de hoogte gehouden van de ontwikkeling van beleid.

Ethische commissies, die onderzoeksvoorstellen beoordelen op ethische maatstaven, worden eveneens maar beperkt meegenomen in het kennisveiligheidsbeleid. 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 hogescholen aan dat ethische beoordeling reeds onafhankelijk van het kennisveiligheidsbeleid is georganiseerd. Bij een paar hogescholen heeft (een lid van) de ethische commissie een (flexibele) rol in het adviesteam Kennisveiligheid.

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).

Een deel van de hogescholen (9 van de 37) geeft aan **bewustwordingscampagnes** te voeren rondom kennisveiligheid, bijvoorbeeld door middel van al bestaande bewustzijnstrainingen over integrale veiligheid, op strategiedagen en via presentaties. Bewustwordingscampagnes zijn vaak eerst gericht op bestuurders en lectoren, in latere fases worden andere onderzoekers en ondersteunend personeel betrokken. Een paar hogescholen houden individuele gesprekken met lectoren van lectoraten waar kennisveiligheid van groter belang is. Een aantal hogescholen geeft aan campagnes momenteel te ontwikkelen. In de verdiepende gesprekken kwam naar voren dat het uitvoeren van de risicoanalyse en het participeren in deze audit ook als startpunten voor bewustwordingsgesprekken werden gebruikt.

Het overgrote deel van de hogescholen (25 van de 37) geeft aan dat binnen hun instelling nog geen procedures zijn specifiek rondom het kennisveiligheidsbewust maken van **HR-medewerkers** (d.w.z. hen in staat stellen om kennisveiligheidsrisico's te signaleren). Van deze groep geven 15 hogescholen aan dat HR-medewerkers bewustzijnstrainingen krijgen over integrale veiligheidsaspecten, zoals privacy en informatie beveiliging, maar dat er binnen deze trainingen geen focus op kennisveiligheid is. Twee hogescholen geen aan wel procedures te hebben, hierbij wordt bijvoorbeeld casuïstiek besproken en flyers gedeeld met het HR-medewerkers. Vijf hogescholen geven aan dat deze procedures in ontwikkeling zijn, twee hogescholen geven aan dat dit onderwerp niet van toepassing is, en van drie hogescholen is dit onbekend.

Het merendeel van de hogescholen (21 van de 37) biedt geen informatie of trainingen gericht op **nieuwe medewerkers** voor de ontwikkeling van kennisveiligheidsbewustzijn. Een deel van de hogescholen (8 van de 37) geeft aan trainingen en bewustzijnscampagnes te hebben, meermaals is het

onderwerp kennisveiligheid ingebed binnen bestaande trainingen over bijvoorbeeld informatie- en cyberveiligheid en privacy. Vier hogescholen geven aan dit momenteel te ontwikkelen, terwijl vier andere hogescholen aangeven dat dit onderwerp niet van toepassing is.

Het overgrote deel van de hogescholen (25 van de 37) biedt (nog) geen opfrismodules voor **zittend personeel**. Een deel van de hogescholen (vijf van de 37) geeft aan dat deze modules wel aanwezig zijn, maar dat deze niet specifiek op kennisveiligheid zijn gericht maar voornamelijk gaan over onderwerpen als informatieveiligheid, privacy en cyberveiligheid. Drie hogescholen geven aan dergelijke opfrismodules nog in ontwikkeling te hebben. Ten slotte geven drie hogescholen aan deze modules niet te hebben en geeft één hogeschool aan dat het onbekend is of ze deze opfrismodules aanbieden.

Geen enkele hogeschool biedt speciale trainingsprogramma's gericht op academische kernwaarden voor **gastdocenten, gaststudenten of gastonderzoekers** uit landen met een verhoogd risicoprofiel. Het grootste deel (28 van de 37) geeft aan dit niet te hebben. Een aantal hogescholen geeft aan dat dit niet van toepassing is (7 van de 37), bijvoorbeeld omdat ze geen gastdocenten of -onderzoekers hebben uit landen met een verhoogd risicoprofiel of dat het risicoprofiel van de hogeschool dit niet vereist. Eén hogeschool geeft aan dat dit in ontwikkeling is en van één hogeschool is het onbekend. Eén hogeschool geeft aan alleen trainingen aan te willen bieden aan alle medewerkers en niet alleen een specifieke doelgroep.

4.1.3 Dienstreizen naar het buitenland

Hogescholen zijn ook gevraagd naar hun beleid rondom dienstreizen naar landen met een verhoogd risicoprofiel. Een deel van de hogescholen heeft hiervoor specifiek beleid (11 van de 37). De hogescholen binnen deze groep geven aan dat dit beleid voornamelijk bestaat uit het volgen van de reisadviezen vanuit het Ministerie van Buitenlandse Zaken.[19] Een aantal hogescholen binnen deze groep kiest ervoor om aanvullende handreikingen en/of procedures op te stellen. Denk hierbij aan advies over het meenemen van ICT-middelen, expliciete toestemming van het College van Bestuur om te reizen naar landen met een oranje of rood reisadvies, of een verplicht goedkeuringsproces. Het grootste deel van de hogescholen geeft aan geen specifiek beleid te hebben (22 uit 37). Bij een aantal hogescholen is het beleid rondom dienstreizen nog in ontwikkeling (vier van de 37).

4.2 Fysieke en digitale beschermingsmaatregelen

Een praktisch punt van aandacht binnen risicomanagement is de toegang tot fysieke en digitale omgevingen van de hogeschool. 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.

4.2.1 Restrictief toegangsbeleid voor ruimtes

Meer dan de helft van de hogescholen (20 van de 37) heeft een **restrictief toegangsbeleid voor bepaalde ruimtes** (zoals afdelingen, gebouwen of labs). Drie hogescholen geven aan dat dit beleid in ontwikkeling is, de overige veertien hogescholen geven aan geen beleid te hebben of dat dit beleid niet van toepassing is. Meerdere hogescholen benoemen dat zij in beginsel openbare instellingen zijn met vrije toegang voor personen, specifiek onderzoekers en studenten, dit principe kwam ook in de verdiepende gesprekken naar voren. Desalniettemin geldt voor een aantal typen ruimtes een restrictief

[19] Reisadviezen | Nederland Wereldwijd

toegangsbeleid. Hier gaat het met name om laboratoria, kantoren en serverruimtes. Dit toegangsbeleid is dan ook meestal niet ontwikkeld vanuit een kennisveiligheidsperspectief, maar dit wordt in toenemende mate meegewogen in het besluit om tot bepaalde ruimtes restrictief toegang te verlenen. Een aantal hogescholen heeft aangegeven hoe deze afweging wordt gemaakt, voor een aantal wordt dit door het hoofd/team ICT gedaan (drie hogescholen) of door de eigenaar van de ruimte (twee hogescholen), andere hogescholen hebben dit niet gespecificeerd.

Van het deel van de hogescholen met een restrictief toegangsbeleid geven elf hogescholen aan beleid te hebben voor de **toegang van buitenlandse reisdelegaties** tot afgesloten ruimtes. Vijf van deze hogescholen geeft aan dat het beleid is dat buitenlandse reisdelegaties alleen toegang krijgen tot restrictieve ruimtes onder begeleiding van een medewerker met toegang tot die ruimte. Vier hogescholen geven aan dat buitenlandse reisdelegaties helemaal geen toegang krijgen tot ruimtes met een restrictief toegangsbeleid. Twee hogescholen hebben niet gespecificeerd hoe dit beleid vorm is gegeven. Vier hogescholen geven aan hier geen beleid voor te hebben, drie hogescholen zeggen dat dit niet van toepassing is op hun instelling en twee hogescholen geven aan dat het beleid in ontwikkeling is. In de verdiepende gesprekken kwam naar voren dat een bezoek van een buitenlandse reisdelegatie meer wordt uitgedacht, van de keuze voor het gebruik van bepaalde ruimtes tot het veilig gebruik van computers en USB-sticks.

4.2.2 Restrictief toegangsbeleid voor onderzoeksgegevens en documenten

Het merendeel van de hogescholen (22 van de 37) geeft aan dat ze beleid hebben omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten. Vaak wordt aangegeven dat dit beleid meer gefocust is op omgang met gevoelige persoonsgegevens dan op kennisveiligheidsrisico's, dit wordt ook onderschreven in de verdiepende gesprekken. Bij veruit de meeste hogescholen is de dataeigenaar verantwoordelijk voor het juist oormerken en omgaan met de data. Veelal is dit de onderzoeker die de data produceert of gebruikt voor onderzoek. Negen hogescholen hebben geen beleid, één hogeschool geeft aan dit beleid in ontwikkeling te hebben. Van één hogeschool is het onbekend en vier hogescholen geven aan dat dit niet van toepassing is. Een deel van de hogescholen (10 van de 37) geeft aan beleid te hebben voor het rubriceren van documenten, denk aan labels als 'vertrouwelijk' of 'geheim'. Dertien hogescholen hebben geen beleid voor het rubriceren van documenten, nog eens elf hogescholen zien dit niet van toepassing op hun instelling. Een enkele hogeschool geeft aan dit beleid in ontwikkeling te hebben (2 van de 37), voor één hogeschool is dit onbekend.

De relevantie van toegang tot digitale omgevingen en data voor kennisveiligheidsbeleid betekent dat er nauwe samenhang is met het **cyberveiligheidsbeleid** van hogescholen. Geregeld zijn medewerkers van cyberveiligheid dan ook betrokken bij kennisveiligheidsbeleid en is de CISO (Chief Information Security Officer) betrokken bij het adviesteam (zie hiervoor 4.1.1). Beide thema's worden gezien als onderdeel van een integrale aanpak binnen de instelling, kennisveiligheid is vaak dan ook ondergebracht in integrale veiligheid. Een deel van de hogescholen geeft aan de samenhang wel te zien, maar deze nog formeel te moeten inrichten. Cyberveiligheid hangt samen met het kennisveiligheidsbeleid, maar wordt niet ontwikkeld als onderdeel van kennisveiligheid met specifieke aandacht voor risicolanden of sensitieve kennis. SURF brengt jaarlijks in beeld wat het cyberdreigingsbeeld[20] is in het hoger onderwijs

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

en voert ook audits[21] uit van het cyberveiligheidsbeleid. In dit sectorbeeld laten we cyberveiligheid daarom verder buiten beschouwing.[22]

4.3 Dilemma's en aandachtspunten

Meerdere hogescholen benoemen 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 hogescholen geven aan dat ze inschatten een **laag risicoprofiel** te hebben, waardoor ze zich afvragen tot op welke hoogte het nodig en proportioneel is om kennisveiligheidsbeleid en procedures te implementeren en onderhouden. Daarbij geven een aantal hogescholen aan dat er belangrijker thema's in ontwikkeling zijn, zoals sociale veiligheid of informatiebeveiliging. Vanwege het ingeschatte lage risicoprofiel geven zij dan minder prioriteit aan kennisveiligheid.

Daarnaast zien meerdere hogescholen de administratieve druk als een dilemma. Kennisveiligheidsbeleid, vastgelegde processen en protocollen kunnen helderheid scheppen voor het signaleren en mitigeren van kennisveiligheidsrisico's. Hogescholen geven echter tegelijkertijd aan dat het beleid niet moet leiden tot een **niet-proportionele bureaucratie** om risico's te beperken. De relevantie en proportionaliteit van kennisveiligheidsbeleid zijn daarom punt van discussie, met name bij de kleinere en monosectorale hogescholen.

4.4 Lessons learned

Meerdere hogescholen zien het aanstellen van een centraal **adviesteam** en/of programmanagers als een goede manier om kennisveiligheid met betrekking tot personeelsbeleid binnen de organisatie te borgen. Adviesteams helpen personeel alert te maken op de kennisveiligheidsrisico's, adviseren over cases, maken risico-inschattingen, vergroten draagvlak binnen de organisatie om met kennisveiligheid aan de slag te gaan en adviseren bij twijfelgevallen. De flexibele schil rondom het adviesteam zorgt voor korte lijnen tussen bijvoorbeeld HR en het adviesteam, wat de werkprocedures en het maken van keuzes bij een twijfelgeval versnelt.

Het draagvlak van kennisveiligheidsbeleid neemt ook toe als beleid binnen de logica van huidige processen op de werkvloer komt te liggen. Verschillende hogescholen combineren kennisveiligheid dan ook binnen overkoepelend beleid op integrale veiligheid, bijv. in combinatie met informatieveiligheid en cyberveiligheid.

---

21 SURFaudit: inzicht en overzicht in je informatiebeveiliging en privacy | SURF.nl

22 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.

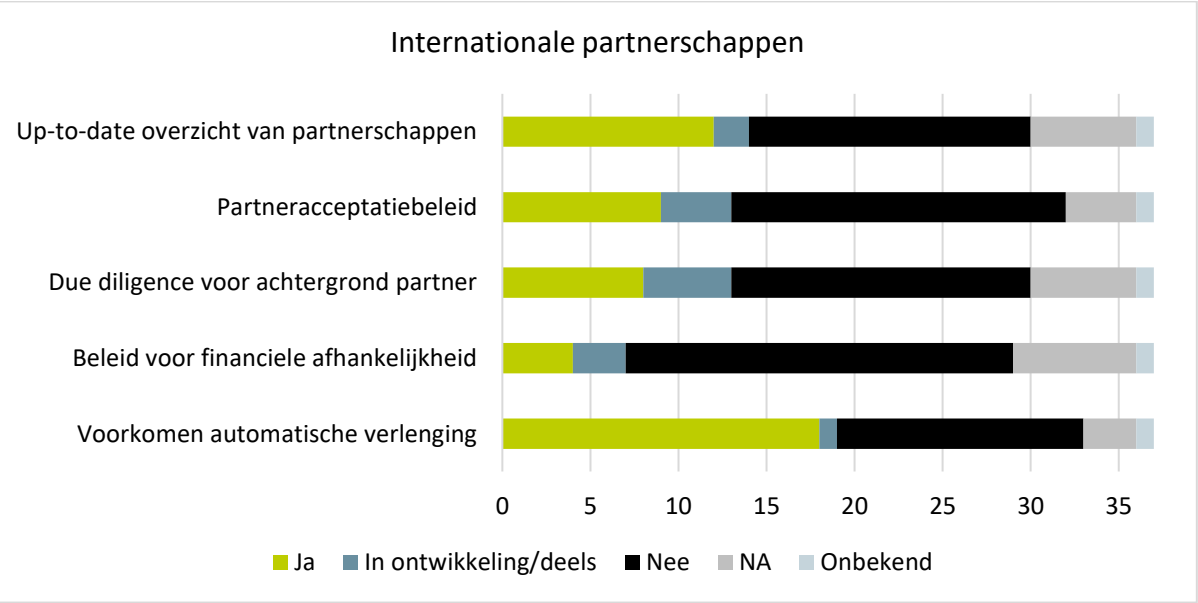
5 Internationale partnerschappen en juridische kaders

In dit hoofdstuk analyseren we het kennisveiligheidsbeleid omtrent internationale samenwerking. Hieronder verstaan we concrete partnerschappen en samenwerkingsverbanden die Nederlandse hogescholen 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 *lessons learned,* dilemma's en aandachtspunten.

5.1 Internationale partnerschappen

Een deel van de hogescholen (9 van de 37) geeft aan geen beleid te hebben rondom internationale partnerschappen en 18 hogescholen geven aan dat dit beleid in ontwikkeling is. Acht hogescholen hebben beleid op internationale partnerschappen: in de volgende paragrafen gaan we in op de verschillende onderdelen van het beleid. Figuur 5.1 geeft een overzicht van de activiteiten van hogescholen ten aanzien van internationale partnerschappen.

Figuur 5.1 Overzicht activiteiten internationale partnerschappen



5.1.1 Centraal overzicht partnerschappen en financiering

Om (instellingsbreed) kennisveiligheidsbeleid te maken op internationale partnerschappen, is het van belang dat er zicht is op de internationale partnerschappen.

Veel hogescholen vinden een dergelijk centraal overzicht niet van toepassing, omdat zij **geen internationale partnerschappen hebben** waarbij samengewerkt wordt op kennisveiligheidsgevoelige thema's. Hierbij spelen verschillende factoren een rol:

- Een deel van hen is (vrijwel) volledig gefocust op onderwijs en niet op onderzoek. Deze hogescholen zijn van mening dat er rondom hun onderwijs geen kennisveiligheidsrisico's spelen. Dit punt wordt zowel in de vragenlijst als in de verdiepende gesprekken genoemd.
- De meeste hogescholen werken vooral samen met regionale partners in Nederland, waar ze ook al een lange professionele relatie mee hebben.
- Ook hogescholen die wel aan onderzoek doen en internationale partnerschappen hebben, geven vaak aan dat de verwachtte kennisveiligheidsrisico's minimaal zijn vanwege de aard van het domein waarin ze werkzaam zijn.

Bij 16 hogescholen is een centraal overzicht van veiligheidsgevoelige partnerschappen niet of nog niet aanwezig en bij twee hogescholen is het in ontwikkeling. Daarnaast geven zes hogescholen aan een overzicht van partnerschappen niet nodig te vinden.

Twaalf hogescholen hebben momenteel wel een overzicht van internationale partnerschappen, al worden kennisveiligheidsrisico's niet altijd in dat overzicht opgenomen. Bij een aantal hogescholen geldt dat elke samenwerkingsovereenkomst altijd op centraal niveau door het CvB wordt ondertekend. Deze centrale overzichten gaan dan voornamelijk over **overeenkomsten rondom onderwijs**, zoals studentuitwisselingen of gezamenlijke opleidingen, omdat veel hogescholen niet of nauwelijks met buitenlandse partners samenwerken aan onderzoek. In de verdiepende gesprekken geeft een hogeschool bijvoorbeeld aan dat ze wel een centraal overzicht van onderwijspartnerschappen heeft, maar nog geen centraal overzicht met internationale onderzoekspartnerschappen.

Daarnaast is de benodigde informatie vaak **gefragmenteerd** aanwezig in de organisatie. Sommige hogescholen hebben een sterk decentrale organisatie, zijn verspreid over meerdere locaties of steden, met veel autonomie op het niveau van instituten, academies of kenniscentra. Als gevolg hiervan hebben zij geen gestandaardiseerde registratie van samenwerkingen in een centraal doorzoekbaar systeem. Een hogeschool noemt dit als een grote barrière, een geeft aan in recente jaren in te zetten op een meer centrale organisatie van het (kennis)veiligheidsbeleid.

Hogescholen geven ook aan dat een samenwerkingscontract soms niet voldoende is om te achterhalen met wie de samenwerking precies gesloten wordt, omdat de ondertekenende partij onderdeel kan zijn van een grotere organisatie of netwerk.

Ten slotte benoemen sommige hogescholen dat het overzicht dat er is actueel wordt gehouden door jaarlijkse controles. Deze hogescholen streven naar een dynamisch overzicht en een meer continue routine waarbij elk partnerschap, inclusief financiering en mogelijke kennisveiligheidsinformatie standaard geregistreerd wordt, waardoor er automatisch een continu up-to-date overzicht ontstaat.

5.1.2 Partneracceptatiebeleid (due diligence)

In deze paragraaf bespreken we hoe het partneracceptatiebeleid van hogescholen eruit ziet, hoe dit proces wordt uitgevoerd en welke *tools* hogescholen hiervoor gebruiken. Negen hogescholen geven aan een partneracceptatiebeleid te hebben. Bij drie hogescholen is dit nog in ontwikkeling; 22 hogescholen geven aan hier (nu) niet mee bezig te zijn. Daarnaast geven acht hogescholen aan dat zij voor mogelijke partners *due diligence* verrichten; vijf hogescholen geven aan dit beleid te ontwikkelen, en 22 hogescholen geven aan dit niet te (gaan) doen.

Veel hogescholen geven aan geen ervaring te hebben met *due diligence* en processen hiervoor niet nodig te vinden, omdat ze weinig tot geen kennisveiligheidsgevoelig onderzoek doen. Bij de meeste hogescholen die wel bezig zijn met een partneracceptatiebeleid is dit ingebed in bestaande afdelingen en teams. Dit gaat dan meestal om de inkoopafdeling, de afdeling juridische zaken of de *international office*. De expertise van deze teams wordt bij een enkele hogeschool standaard ingezet bij samenwerking met partners van buiten de EU. Een paar hogescholen hebben een adviseur kennisveiligheid aangenomen die hier ook een rol in speelt. Bij de hogescholen die een partneracceptatiebeleid hebben, ligt de uiteindelijke tekenverantwoordelijkheid meestal bij de CvB. Bij sterk decentraal georganiseerde hogescholen kunnen er ook op dat decentrale niveau partnerschappen worden afgesloten. Een enkele hogeschool geeft aan beleid te ontwikkelen rondom ethische overwegingen (rondom o.a. duurzaamheid, rechtvaardigheid en inclusie) tijdens samenwerking met externe partners.

Als *due diligence* op kennisveiligheidsgebied nodig is, moet eerst een (potentieel) kennisveiligheidsrisico gesignaleerd worden. Deze signalerende functie ligt bij hogescholen momenteel meestal bij het formele ondertekenen van de overeenkomst, dus bij de inkoopafdeling of bij juridische zaken. Van individuele onderzoekers wordt dit momenteel in mindere mate verwacht. Hogescholen vinden het wel belangrijk dat lectoren en onderzoekers kennisveiligheidsbewust zijn, en geven aan dit bewustzijn bij onderzoekers wel te willen verhogen. In de verdiepende gesprekken geeft een hogeschool aan momenteel een checklist voor samenwerking rondom onderzoek te ontwikkelen, die door onderzoekers ingevuld moet worden voor de samenwerking aangegaan wordt.

Als een mogelijk risico gesignaleerd wordt, schakelen hogescholen die dat hebben hun adviseur kennisveiligheid in voor advies over een aangaan van een mogelijke samenwerking. Een enkele hogeschool heeft daarnaast gebruik gemaakt van het Loket Kennisveiligheid om advies te krijgen over een lopende samenwerking die de hogeschool risicovol vond.

Hogescholen wegen de mate waarin er financiële, reputatie-gerelateerde of juridische consequenties aan een partnerschap verbonden (kunnen) zijn. Potentiële samenwerkingsverbanden worden beoordeeld op:

- De inhoud van de samenwerking, bestaande uit:
    - De mate waarin het onderzoek aansluit bij de strategische onderzoeks- en onderwijsdoelen van de hogeschool.
    - De normen en waarden van de hogeschool.
    - Juridische bepalingen (zie paragraaf 5.2).
- De samenwerkingspartner. Hogescholen letten hier op de veiligheid in het land van herkomst van de samenwerkingspartner, waarbij ze gebruik maken van informatie en reisadviezen van het ministerie van Buitenlandse Zaken. Hogescholen beoordelen hoe het land scoort op de gebieden van rechtsstatelijkheid en academische vrijheid. Waar mogelijk wegen hogescholen resultaten van reeds bestaande samenwerking met deze partner.

In het proces van *due diligence* maken hogescholen gebruik van meerdere bronnen en tools, waaronder:

- Een interne checklist met (kennis)veiligheidsrisico's
- Sanctiewetgeving EU
- Website Buitenlandse Zaken en score land op rechtsstatelijkheid
- Internationale ranglijsten m.b.t. academische vrijheid
- Eén hogeschool geeft in de verdiepende gesprekken aan de ASPI-tracker te gebruiken.

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. Vier hogescholen geven aan beleid te hebben rondom dit thema, en drie zijn dit aan het ontwikkelen. Qua maatregelen om financiële afhankelijkheid te voorkomen zetten hogescholen veelal in op bewustwording en niet op geformaliseerde processen. Hogescholen noemen ook dat *checks and balances* plaatsvinden, doordat alle financiële verplichtingen door het CvB ondertekend moeten worden.

29 hogescholen geven aan geen beleid te hebben om te voorkomen dat ze in een staat van financiële afhankelijkheid worden gebracht. Een expliciete reden die veel van deze hogescholen geven om geen beleid te hebben, is dat externe financiering een beperkt deel uitmaakt van hun totale financiering. Zo was tussen 2012 en 2018 minder dan 1% van de inkomsten van hogescholen afkomstig van financiering van internationale organisaties, nationale overheden, overige non-profitorganisaties en bedrijven.[23] Dit deel is zo klein dat het niet mogelijk is om op instellingsniveau financieel afhankelijk te worden van een enkele externe financier.

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. Achttien hogescholen geven aan dat ze beleid hebben om automatische verlenging van internationale partnerschappen te voorkomen, één hogeschool is dit aan het ontwikkelen. Zeventien hogescholen geven aan zulk beleid niet te hebben en ook niet te gaan ontwikkelen.

De meeste samenwerkingsverbanden kennen een formeel contract, en meerdere hogescholen doen aan (een vorm van) contractmanagement, waarbij automatisch een notificatie wordt afgegeven als een contract bijna afloopt. Sommige hogescholen spreken de ambitie uit om dit verder uit te breiden met de implementatie van vaste evaluatiemomenten; één hogeschool werk aan een beleidskader voor partners voor studentmobiliteit. Sommige hogescholen geven aan nooit contracten voor onbepaalde tijd contracten met stilzwijgende verlenging af te sluiten.

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.

[23] Rathenau Instituut (2020). Ontwikkeling derde geldstroom en beïnvloeding van wetenschappelijk onderzoek – Een data- en literatuuronderzoek ter beantwoording van de motie-Westerveld. Den Haag (auteurs: Broek-Honingh van den, N., M. Schel en A. Vennekens).

Hogescholen geven in grote mate aan dat dit soort technologie niet wordt onderzocht of ontwikkeld aan hun instelling. Bovendien heeft de verordening betrekking op (de beperking van) de export van dual-use-technologie buiten de EU,[24] terwijl *als* hogescholen al dual-use-technologie onderzoeken of ontwikkelen dit nauwelijks gebeurt met partners buiten de EU. Dit juridische kader is daarom voor hen niet relevant en er is geen beleid benodigd voor compliance. Enkele hogescholen bij wie dit wel speelt, geven aan een jaarlijkse inventarisatie te maken van mogelijke dual-use technologieën.

Daarnaast geven hogescholen zowel in de vragenlijst als in de verdiepende gesprekken aan dat voor compliance gespecialiseerde juridische kennis nodig is. Omdat dual-use compliance bij hogescholen relatief beperkt voorkomt, is het voor hen niet rendabel om die gespecialiseerde kennis continue in huis te hebben. Hogescholen geven in de verdiepende gesprekken aan meer te zien in samenwerking tussen hogescholen, zodat deze gespecialiseerde kennis bij meerdere hogescholen te gebruiken is. Deze samenwerking komt volgens één hogeschool tot nu toe onvoldoende tot stand. Zo geven meerdere hogescholen in verdiepende gesprekken aan dat er nog geen lessen rondom casuïstiek worden uitgewisseld, geen beleidsoverleg is en ook geen specialistische kennis wordt gedeeld. De voornaamste reden die zij hiervoor geven is de grote diversiteit in hogescholen die ervoor zorgt dat kennisveiligheidsproblematiek niet overal even belangrijk wordt gevonden.

Hogescholen bij wie compliance met exportcontroles van dual-use technologie speelt geven aan dat de borging van dual-use compliance momenteel ad-hoc is. Als zich een casus aandient zoeken hogescholen intern of extern naar de benodigde kennis, maar daar zijn geen standaard procedures voor.

5.2.2 Compliance met niet-EU import- en exportregels

Ook landen buiten de EU hebben import- en exportregels die voor Nederlandse hogescholen relevant kunnen zijn. Hogescholen geven echter bijna unaniem aan dat deze regels voor hen niet relevant zijn.

5.2.3 Compliance met internationale en EU-sanctieregimes

Weinig hogescholen hebben beleid over hoe te voldoen aan internationale sanctieregimes. Sommige hogescholen geven aan dat dit case-by-case door het CvB wordt behandeld. Bij sommige hogescholen is compliance wel belegd bij de inkoopafdeling of bij juridische zaken. Hogescholen met een adviesteam kennisveiligheid, betrekken dat team hier bij. Een enkele hogeschool geeft aan dat kennisveiligheidsbewustzijn onder personeel een belangrijk instrument voor compliance is. Verder volgen hogescholen vooral het beleid en de informatievoorziening van de Nederlandse Rijksoverheid, via publicaties en de website van het ministerie van Buitenlands Zaken.

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[25], de Nederlandse Gedragscode Wetenschappelijk Integriteit[26] (NGWI) en de EU guidelines on Tackling R&I foreign interference[27]. Veel hogescholen vinden deze niet op hen van toepassing, en gebruiken ze dan ook niet. Hogescholen die deze gedragscodes wel gebruiken doen dit op incidentele basis of bespreken hoe ze dat structureel kunnen gaan doen. Deze hogescholen noemen vaak de NGWI als een gedragscode die onderschreven en structureler toegepast wordt.

---

24 EUR-Lex - 32021R0821 - EN - EUR-Lex (europa.eu)

25 VSNU Kader Kennisveiligheid Universiteiten.pdf (universiteitenvannederland.nl)

26 https://www.nwo.nl/nederlandse-gedragscode-wetenschappelijke-integriteit

27 Tackling R&I foreign interference - Publications Office of the EU (europa.eu)

5.3 Dilemma's en aandachtspunten

Op het vlak van internationale partnerschappen en juridische kaders speelt een aantal dilemma's en aandachtspunten. Veel hogescholen vinden dat de problematiek rondom partnerschappen en kaders bij hun weinig voorkomt. Een aanzienlijk deel van de hogescholen heeft amper tot geen internationale of onderzoekspartnerschappen. Bij hogescholen die dit wel hebben, heeft samenwerking zelden kennisveiligheidsrisico's. Hierdoor is het **niet proportioneel** om de benodigde kennis in huis te hebben. Hogescholen zouden hier meer onderling en/of met universiteiten op kunnen samenwerken en dit soort kennis delen.

Internationale partnerschappen worden op hogescholen veelal beoordeeld op basis van hun contractvorm of -inhoud, door **de inkoopafdeling of door juridische zaken**. Hier is zelden een adviesteam kennisveiligheid bij betrokken. Daarnaast rijst de vraag op deze benadering voldoende is om precies te achterhalen met wie er samengewerkt wordt.

Voor compliance met **juridische kaders** geldt dat dit afhankelijk is van individuele onderzoekers voor het signaleren van onder meer (risico's op) dual-use toepassingen van hun onderzoek. Onderzoekers zijn vaak beperkt op de hoogte van de juridische kaders. Deze kennis bij elkaar brengen vraagt aandacht.

Ten slotte zien we dat ook bij internationale samenwerkingsverbanden de aandacht voornamelijk uitgaat naar kennisveiligheid in de context van sensitieve kennis en technologie. Kennisveiligheidsrisico's ten aanzien van **heimelijke beïnvloeding en ethische kwesties** krijgen nog beperkte aandacht in het beleid op het aangaan van samenwerkingsverbanden.

5.4 Lessons learned

Kennisveiligheid in internationale samenwerking en compliance met juridische kaders laat zich niet goed vatten in afvinklijstjes. Dit wordt al genoemd in het AWTI-rapport en wordt ook door hogescholen beaamd. Gezien de soms beperkte casuïstiek zijn hogescholen bezorgd over onnodige bureaucratie. Hogescholen noemen daarom bewustwording als een belangrijk onderdeel van hun toekomstig beleid. Hogescholen willen echter ook geen overbewustzijn creëren. Er is bij hogescholen maar een (zeer) beperkt aantal medewerkers voor wie kennisveiligheid speelt, zij moeten bewust zijn. Hogescholen geven aan dat ongerichte bewustwordingscampagnes mogelijk leiden tot paranoia en stigmatisering.

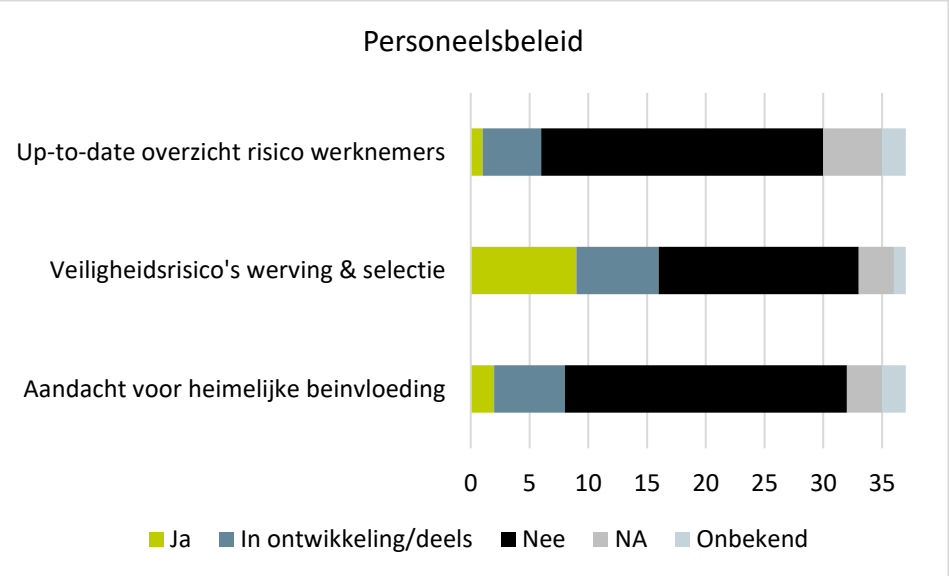
6 Personeelsbeleid

De Leidraad stelt dat het wenselijk is dat kennisveiligheid onderdeel wordt van het personeelsbeleid. In dit hoofdstuk beschrijven we eerst op welke manier kennisveiligheid is geïmplementeerd in verschillende onderdelen van het personeelsbeleid van de hogescholen. 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 instellingen op dit vlak hebben geleerd.

6.1 Vertaling kennisveiligheid in personeelsbeleid

Minder dan de helft van de hogescholen (15 van de 37) geeft aan dat kennisveiligheid geen onderdeel is van het personeelsbeleid. Vijftien andere hogescholen geven aan dat het kennisveiligheidsbeleid met betrekking tot personeelsbeleid nog in ontwikkeling is, of dat het beleid is vastgesteld en de uitvoering aantoonbaar is. Drie hogescholen geven aan dat er een verbetercyclus aanwezig en gedocumenteerd is. Twee hogescholen geven aan een instellingsbreed risico- en beheersprogramma te hebben waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus (zie eerder Tabel 2.1). Zie Figuur 6.1 voor een overzicht van kennisveiligheidsactiviteiten rondom personeelsbeleid van hogescholen.

Figuur 6.1 Overzicht activiteiten personeelsbeleid



6.1.1 Overzicht (gast)werknemers

We vroegen hogescholen in hoeverre zij op bestuursniveau een centraal en up-to-date overzicht hebben van werknemers, gasten en gastwerknemers *die een risico vormen op het gebied van kennisveiligheid*. 24 van de 37 hogescholen gaven nadrukkelijk aan dit niet te doen. De redenen die hogescholen aandragen om geen centraal overzicht bij te houden lopen uiteen. Twee hogescholen geven in de toelichting aan zich sterk af te vragen of het privacytechnisch verantwoord is om een centraal overzicht op te stellen van potentiële risicovolle werknemers, gasten en gastwerknemers. Andere hogescholen

geven aan (nog) geen overzicht bij te houden, omdat er binnen de instelling nog geen kennisveiligheidsbeleid is, het ontbreekt aan landelijke kaders, of omdat het bijhouden van een overzicht volgens de betreffende instelling niet nodig is.

Zes hogescholen geven aan op centraal niveau wel (gedeeltelijk) overzicht bij te houden van de (gast)werknemers. Drie hogescholen geven daarbij expliciet aan niet bij te houden wie van deze werknemers een risico vormt voor kennisveiligheid.

6.1.2 Werving en selectieprocedure

Negen van de 37 hogescholen geven aan in meer of mindere mate veiligheidsrisico's mee te wegen bij de werving en selectie van nieuwe medewerkers. Zij volgen formele of informele procedures en richtlijnen, en/of controleren (een deel) van het nieuwe personeel op mogelijke kennisveiligheidsrisico's middels het toetsen van zijn of haar achtergrond. Deze hogescholen vragen veelal om een Verklaring Omtrent het Gedrag (VOG), en vullen dit aan met een referentiecheck, een check op getuigschriften en/of een achtergrondscreening. Eén hogeschool geeft aan kandidaten uit een land met potentiële veiligheidsrisico's individueel af te wegen. Een andere hogeschool geeft aan het Loket Kennisveiligheid te raadplegen in geval van twijfel over een nieuwe medewerker. Een klein deel van de hogescholen geeft aan überhaupt zeer weinig tot geen medewerkers uit risicolanden in dienst te hebben, en vragen zich af in hoeverre het zinvol is om uitgebreid personeelsbeleid ten aanzien van kennisveiligheid op te tuigen.

Zeventien hogescholen wegen kennisveiligheidsrisico's niet mee bij de werving en selectie van nieuwe medewerkers. Zij doen dit omdat zij geen risico's hebben gesignaleerd voor kennisveiligheid, of omdat de uitgangspunten ten aanzien van kennisveiligheid voor de werving en selectiefase nog in ontwikkeling zijn. Uit de verdiepende gesprekken met in ieder geval één instelling blijkt dat dit niet betekent dat er helemaal geen aandacht is voor sollicitanten uit risicolanden. In een dergelijk geval volgt de kandidaat dezelfde sollicitatieprocedure als alle andere sollicitanten, maar zijn medewerkers rondom deze sollicitant alerter op afwijkende signalen.

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. Hogescholen zijn zich bewust van de risico's op heimelijke beïnvloeding. Echter geeft het overgrote merendeel van de hogescholen (24 van de 37) aan geen specifiek beleid te hebben voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding. Een aantal hogescholen die geen specifiek beleid hebben ontwikkeld rondom heimelijke beïnvloeding, of (nog) geen aandacht aan dit onderwerp besteedt, geeft expliciet aan dat er in de risicoanalyse geen risico's op heimelijke beïnvloeding zijn gesignaleerd of dat zij geen medewerkers uit risicolanden in dienst hebben. Een deel van deze hogescholen besteedt wel aandacht aan het thema, maar heeft nog geen beleid opgesteld. Slechts één hogeschool geeft in de toelichting expliciet aan beleid te hebben opgesteld om de sociale veiligheid van alle studenten en medewerkers te monitoren en te borgen.

Ook uit de verdiepende gesprekken met de hogescholen maken we als onderzoekers op dat er (nog) weinig aandacht is voor heimelijke beïnvloeding. Eén hogeschool geeft in de gesprekken aan dat er door de aard van de kennis die zij in huis hebben geen sprake is van veiligheidsrisico's. Het risico op heimelijke beïnvloeding voor het personeel is volgens hen dan ook gering. Er wordt volgens deze hogeschool ook niet actief gemonitord op dit thema, of gesprekken gevoerd over heimelijke

beïnvloeding met een kandidaat-medewerker. Tegelijkertijd laat de organisatie weten dat heimelijke beïnvloeding altijd op de loer ligt wanneer een onderzoeker persoonlijk belang heeft bij een onderzoek en collega's chanteert. Wel vraagt de organisatie zich af hoe de controle op heimelijke beïnvloeding kan worden uitgevoerd naast de huidige achtergrondtoetsing voor samenwerkingen en voor nieuwe medewerkers en hoe de inlichtingendiensten hier eventueel bij kunnen ondersteunen.

6.2 Dilemma's en aandachtspunten

Een aantal hogescholen 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 Discriminatie en uitsluiting

Vier hogescholen geven aan dat het in de opzet, afstemming en uitvoering van personeelsbeleid op het gebied van kennisveiligheid van groot belang is om discriminatie en stigmatisering te voorkomen, en dat het generiek weren van mensen met een specifieke nationaliteit wettelijk niet toegestaan is (discriminatieverbod).[28]

Deze hogescholen geven aan zich zorgen te maken over de spagaat tussen het borgen van kennisveiligheid enerzijds, en het risico op discriminatie anderzijds. Eén hogeschool noemt dat het opvragen van de nationaliteit en/of het geboorteland van een medewerker alleen kan met opgaaf van goede reden. De risicoanalyse op kennisveiligheid is volgens deze instelling (nog) geen geaccepteerde reden. Het opzoeken van deze gegevens of het nadrukkelijk vragen naar deze gegevens werkt volgens deze hogeschool profilering op basis van voornaam of achternaam in de hand. Een andere hogeschool geeft hierop aan dat personeelsbeleid zich in de achterhoede bevindt qua inspanningen op het gebied van kennisveiligheid. Deze hogeschool geeft aan de discussie rondom screening in het kader van kennisveiligheid op de voet te volgen, maar vindt het niet verstandig om daarop vooruit te lopen.

Dat hogescholen zich bewust zijn van het risico op discriminatie horen we ook terug wanneer één van de hogescholen in de verdiepende gesprekken aangeeft bang te zijn om in de media te worden weggezet als discriminerende organisatie. In ieder geval twee hogescholen noemen in de verdiepende gesprekken dat gesprekken over kennisveiligheid niet alleen met kandidaten uit risicolanden zouden moeten worden gevoerd, maar met alle sollicitanten.

6.2.2 Achtergrondtoetsing[29]

Het toetsen van de achtergrond van nieuw personeel is voor veel hogescholen een heet hangijzer. Zo maken we uit de gesprekken op dat hogescholen zoekende zijn in de mate waarin ze nieuw personeel al dan niet moeten en willen toetsen op hun achtergrond. Zeker nu er nog geen kader is voor achtergrondtoetsing zoeken meerdere hogescholen naar toetsingsbeleid dat passend is bij de organisatie en binnen bestaande wetgeving. Daarbij uit één hogeschool juridische en ethische twijfels als belemmering voor achtergrondtoetsing. Het uitvoeren van een achtergrondtoets van nieuw

---

[28] Hierbij wordt verwezen naar het oordeel in cassatie door de Hoge Raad over de Nederlandse Sanctieregeling Iran 2012 (zie ECLI:NL:HR:2012:BX8351, voorheen LJN BX8351, Hoge Raad, 11/03521 (rechtspraak.nl))

[29] Hogescholen 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.

personeel kan volgens een andere hogeschool daarnaast een stigmatiserende uitwerking hebben op het personeel.

In ieder geval twee hogescholen geven aan dat kennisveiligheidsrisico's in principe voor iedere nieuwe medewerker gelden, en niet alleen voor kandidaten uit risicolanden. Een andere hogeschool geeft daarnaast ook aan het niet als hun verantwoordelijkheid te zien om te bepalen welke studenten al dan niet getoetst moeten worden, en laat dit liever aan instanties als de Immigratie- en Naturalisatiedienst (IND). De IND speelt immers al een centrale rol bij het verlenen van werkvergunningen aan personeel van buiten de EU in Nederland.

6.2.3 Minimale vertegenwoordiging risicolanden

Zowel in de zelfevaluatie als in de verdiepende gesprekken geven hogescholen aan dat het aantal medewerkers uit risicolanden binnen hun organisatie zeer gering is. Zo geeft een betrokkene van één hogeschool in de casestudies als voorbeeld dat er momenteel slechts twee medewerkers uit een potentieel risicoland binnen de hogeschool actief zijn. Ook een andere hogeschool geeft aan dat er jaarlijks weinig tot geen sollicitanten zijn uit risicolanden. Daarom geven beide hogescholen aan weinig animo te hebben voor het invoeren van uitgebreid personeelsbeleid met betrekking tot kennisveiligheid.

6.3 Lessons learned

6.3.1 Toetsing alle nieuwe kandidaten

Meerdere hogescholen geven in de zelfevaluatie en in de verdiepende gesprekken aan het ethisch onwenselijk te vinden om achtergrondtoetsing uit te voeren op basis van nationaliteit. Om te voorkomen dat kandidaten bij voorbaat worden uitgesloten op basis van hun nationaliteit, geeft één hogeschool als oplossing aan alle kandidaten uit het buitenland te willen toetsen op hun achtergrond. Op die manier wordt geen onderscheid gemaakt naar achtergrond, en loopt de instelling een minder groot risico op stigmatisering en discriminatie. Het nadeel is wel dat de werklast daarmee wordt verhoogd. In een ander verdiepend gesprek wordt hierop echter aangegeven dat het aantal sollicitanten uit het buitenland op onderzoeksfuncties dermate beperkt is, dat de werklast naar verwachting beperkt blijft.

7 Conclusie en aandachtspunten

In dit hoofdstuk geven we een beknopte hoofdconclusie ten aanzien van het sectorbeeld kennisveiligheid hogescholen, namelijk dat het beleid nog in ontwikkeling is, maar niet bij alle hogescholen als relevant wordt gezien. Daarnaast concluderen we dat hogescholen tegen een aantal dilemma's aanlopen die van invloed zijn op de ontwikkeling van het kennisveiligheidsbeleid. Tot slot presenteren we twee aandachtspunten voor de verdere ontwikkeling van het nationale kennisveiligheidsbeleid.

7.1 Conclusie: beleid in ontwikkeling, maar niet overal relevant

Het belang van het kennisveiligheidsbeleid wordt door hogescholen verschillend ervaren. In het algemeen staat kennisveiligheid minder hoog op de agenda dan andere onderdelen van integrale veiligheid, zoals sociale veiligheid of informatiebeveiliging. Dit heeft te maken met twee aspecten. Ten eerste zijn hogescholen in sterke mate gericht op onderwijs en minder op onderzoek. Er is in het algemeen minder sprake van onderzoekssamenwerking met andere kennisinstellingen, van kroonjuwelen of van onderzoek op sensitieve kennisgebieden. Ten tweede vind onderzoek vaker plaats in samenwerking met maatschappelijke en kennispartners uit de regio of Nederland dan met partners buiten de EU, waardoor kennisveiligheid vanzelfsprekend minder speelt. Internationale samenwerking gebeurt voornamelijk op onderwijs (zoals mobiliteit van studenten), maar hierin ervaren hogescholen geen kennisveiligheidsrisico's.

De grotere brede hogescholen erkennen desalniettemin het belang van het voeren van beleid op kennisveiligheid en hebben meestal beleid ontwikkeld of zijn dat aan het doen. Bij deze hogescholen is het kennisveiligheidsbeleid doorgaans vanaf 2022 op de agenda gekomen. Van de hogescholen die in 2022 de risicoanalyse op verzoek van de minister hebben uitgevoerd, was dit voor het overgrote deel hun eerste ervaring met kennisveiligheid. Bij een aantal hogescholen zijn nieuwe risico's ontdekt en daarna ook concrete maatregelen getroffen. Deze hogescholen zijn sindsdien actief bezig om de adviezen van de Leidraad vorm te geven.

Een aantal hogescholen voert bewust geen kennisveiligheidsbeleid. Dit zijn veelal kleinere en monosectorale hogescholen. Zij vinden het niet relevant om kennisveiligheidsbeleid te ontwikkelen, omdat zij ofwel geen sensitief onderzoek doen, geen internationale partnerschappen hebben, of geen buitenlandse werknemers en studenten hebben.

De hogescholen hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel 7.1). Ook hierin zien we terug dat een deel van de hogescholen op diverse onderdelen geen kennisveiligheidsbeleid ontwikkelt; bij de andere hogescholen is het kennisveiligheidsbeleid nog veelal in ontwikkeling. Daarnaast 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.
- De aspecten juridische kaders en personeelsbeleid ontbreken relatief vaker dan de andere onderdelen in het kennisveiligheidsbeleid van hogescholen.
- Kennisveiligheid wordt door een aantal hogescholen gezien als onderdeel van algemeen risicomanagement, integrale veiligheid of cyberveiligheid. Zij geven daarom aan op die onderdelen

wel vaststaand instellingsbreed beleid (en dus een hoge score in de rubric) te hebben, dat echter niet specifiek is toegespitst op *kennis*veiligheid.

Tabel 7.1. Zelfscores in de fase van beleidsontwikkeling. Verschillende hogescholen hebben op één of meer onderdelen geen score ingevuld. Hierdoor is de n per onderwerp minder dan 37.

	Geen beleid	Gedeelten van beleid in ontwikkeling	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 verbetercyclus aanwezig	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Risicoanalyse	10		17		4		2	2
Risicomanagement	9		17	1	4		1	2
Fysieke en digitale beschermings-maatregelen	8	1	13	2	9	1	1	1
Internationale partnerschappen	9		18		5	1	1	1
Juridische kaders	18		15		1			1
Personeelsbeleid	15		9	1	5	1	2	2

7.2 Dilemma's

In het ontwikkelen en uitvoeren van kennisveiligheidsbeleid zien we een aantal dilemma's en aandachtspunten bij de hogescholen die van belang zijn voor het landelijke debat over kennisveiligheidsbeleid.

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 hogescholen die in de regel geen nieuwe technologie ontwikkelen of fundamenteel onderzoek doen. Meerdere hogescholen geven aan dat ze inschatten een **laag risicoprofiel** te hebben, waardoor ze zich afvragen 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. Hogescholen geven echter tegelijkertijd aan dat het beleid niet moet leiden tot een **niet-proportionele bureaucratie** om risico's te beperken. Hierbij speelt ook de grote diversiteit tussen hogescholen.

7.3.4. De hogeschool 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 hogescholen moet worden meegewogen. Hogescholen werken in hun praktijkgericht onderzoek samen met bedrijven die wellicht actief zijn op sensitieve kennisgebieden. Ook lopen studenten stages bij bedrijven en instituten waar kennisveiligheid een belangrijke overweging kan zijn. Hoewel bedrijven en instituten in principe zelf

verantwoordelijk zijn voor hun eigen kennisveiligheidsbeleid, geven enkele hogescholen aan dat ook zij verantwoordelijkheid dragen als toegangspoort tot hun (regionale) netwerk.

7.2.2 Samenwerking centraal en decentraal

Een aantal hogescholen is nog zoekende in de samenwerking tussen de centrale en decentrale niveaus. Het centrale bestuur zoekt naar een balans tussen het creëren van bewustzijn en analyseren van potentiële risico's bij *alle* afdelingen, wat kan leiden tot paranoia, discriminatie of irritatie, en beleid gericht op *specifieke* afdelingen, waardoor bepaalde medewerkers of afdelingen wellicht onvoldoende bewust raken van kennisveiligheid.

7.3 Aandachtpunten

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

Ten eerste ontwikkelt een groot aantal hogescholen geen kennisveiligheidsbeleid omdat zij aangeven dat er op hun instelling geen kennisveiligheidsrisico's spelen. Een risico hierbij is dat met onvoldoende ontwikkelde **expertise** het ook niet goed mogelijk is **om kennisveiligheidsrisico's te signaleren**. Een aandachtspunt is dus dat hogescholen goed in staat dienen te worden gesteld om kennisveiligheidsrisico's te detecteren, zonder een disproportioneel apparaat te ontwikkelen voor kennisveiligheidsbeleid voor de omgang met eventuele kennisveiligheidsrisico's.

Ten tweede, hiermee samenhangend, zijn er kansen voor (intensiever) **samenwerking tussen hogescholen onderling** en met universiteiten. Zeker waar het niet proportioneel is voor elke hogeschool om expertise te ontwikkelen, kan het nuttig zijn om in sterkere mate samen te werken. Hierbij valt bijvoorbeeld te denken aan een gezamenlijk Adviesteam Kennisveiligheid, uitwisseling van geleerde lessen en kennisdeling voor het uitvoeren van risicoanalyses.

Bijlage 1 Vragenlijst

Kennisveiligheid

1. Hoe wordt het begrip 'kennisveiligheid' binnen uw instelling gedefinieerd?
2. Sinds wanneer is er sprake van het ontwikkelen, vaststellen of uitvoeren van beleid op kennisveiligheid aan uw instelling?

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[30]. In deze vragenlijst maken we onderscheid tussen deze risicoanalyse op verzoek van de minister, en risicoanalyses die uw instelling uitvoert als onderdeel van regulier beleid (volgend blok).

3. Kunt u toelichten of u deze risicoanalyse heeft uitgevoerd en hoe u deze heeft vormgegeven?
4. Heeft de oproep van de minister geleid tot nieuwe of andere activiteiten in vergelijking met eventuele risicoanalyses die uw instelling al uitvoerde als onderdeel van het eigen kennisveiligheidsbeleid? Kunt u dit toelichten?
5. Heeft uw instelling 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)?
6. Heeft uw instelling bij deze risicoanalyse gebruik gemaakt van advies van het Loket Kennisveiligheid of contact gehad met de contactpersoon van uw instelling bij de veiligheidsdiensten?
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)
8. Hebben de uitkomsten van deze risicoanalyse geleid tot concrete maatregelen (u hoeft de maatregelen zelf 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?

Het inschatten van risico's

De volgende vragen gaan in op de risicoanalyses die uw instelling uitvoert als onderdeel van het eigen kennisveiligheidsbeleid. Indien dit eerder niet het geval was en uw instelling alleen ervaring heeft met de risicoanalyse in reactie op de oproep van de minister kunt u onderstaande vragen voor die specifieke risicoanalyse beantwoorden.

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

10. Kunt u het huidige kennisveiligheidsbeleid van uw instelling 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 instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Het inschatten van risico's					

11. Maken risicoanalyses op kennisveiligheid al langer onderdeel uit van het reguliere beleid van uw instelling (eventueel onder andere terminologie)?
    - Ja, dat doen we op centraal niveau
    - Ja, dat doen we op decentraal niveau
    - Ja, dan doen we op zowel centraal als decentraal niveau
    - Nee, de risicoanalyse n.a.v. de oproep van de minister is onze eerste ervaring hiermee
    - Anders, namelijk
12. We zijn benieuwd op welke manier uw instelling risicoanalyses voor kennisgebieden maakt. Kunt u dit aan de hand van onderstaande vragen beschrijven?
    a) Worden sensitieve kennisgebieden binnen uw instelling geïdentificeerd? Zo ja, wie doet dat en op welk moment vindt die analyse plaats?
    b) Hanteert uw instelling een eigen lijst met sensitieve kennisgebieden? Zo ja, kunt u toelichten hoe deze tot stand komt en hoe uw instelling zorgt dat deze actueel blijft?
    c) Op welke manier bepaalt uw instelling of onderwijs of onderzoek onder deze kennisgebieden valt?
    d) Brengt uw instelling daarbij de 'kroonjuwelen' in kaart? In de Leidraad wordt dit gedefinieerd als kennisgebieden waarbij kennisveiligheidsrisico's zijn verbonden aan kennisoverdracht en waarop uw instelling internationaal toonaangevend is. Zo ja, kunt u toelichten hoe dit wordt gedaan?
13. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met partnerorganisaties of personen uit specifieke landen:
    a) Hoe doet uw instelling 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 instelling, instituten, onderzoekers of projectleiders de samenwerking met buitenlandse partnerorganisaties of opdrachtgevers beoordelen? Zo ja, wat is hierin veranderd en wat was hiervoor de aanleiding?
14. Zijn er binnen uw instelling 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 instelling hier dan mee omgaat?
15. Heeft u verder nog opmerkingen of een toelichting ten aanzien van het inschatten van risico's?

Organisatie risicomanagement

De volgende vragen gaan in op de organisatie van risicomanagement op het gebied van kennisveiligheid binnen uw instelling. Kennisveiligheid kan belegd zijn bij verschillende afdelingen of bij verschillende verantwoordelijken. Om een beeld te krijgen hoe instellingen dit organiseren vragen we graag voor verschillende afdelingen of zij een rol spelen in het kennisveiligheidsbeleid van uw instelling.

16. Kunt u het huidige kennisveiligheidsbeleid van uw instelling met betrekking tot de organisaties van het risicomanagement kennisveiligheid scoren aan de hand van onderstaande rubric?

	Geen beleid	Beleid is nu in ontwikkeling	Beleid is vastgesteld en de uitvoering is aantoonbaar	Er is een verbetercyclus aanwezig en gedocumenteerd	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Risicomanagement					

17. Is er binnen uw instelling op bestuurlijk niveau een portefeuillehouder kennisveiligheid?
18. Heeft uw instelling een Adviesteam Kennisveiligheid? Kunt u achtergrond, deskundigheid en samenstelling van dit team beschrijven?
19. Op welke wijze wordt beleidsmatige afstemming verkregen tussen het instellingsbrede kennisveiligheidsbeleid en de decentrale onderdelen (zoals faculteiten, instituten, academies)?
20. In welke mate spelen de ethische commissie(s) (of ethical review board) binnen uw instelling een rol in het kennisveiligheidsbeleid? (Bijvoorbeeld: kunnen ze adviseren en/of goedkeuren over ethisch gebruik van onderzoeksresultaten?)
21. Zijn er vertrouwenspersonen of kennisloketten binnen uw instelling waar medewerkers terechtkunnen met signalen en vragen over veiligheidsrisico's?
22. Hebben technology/knowledge transfer office(s) en accelerators/startup academies binnen uw instelling 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 instelling niet beschikt over een technology/knowledge transfer office of accelators/startup academies graag "n.v.t." invullen)[31]
23. Zijn er nog andere functionarissen of organen binnen uw instelling betrokken bij het beleid op kennisveiligheid? Zo ja, om welke functies gaat dit en welke rol spelen zij?
24. Heeft u verder nog opmerkingen of een toelichting ten aanzien van de organisatie van risicomanagement op kennisveiligheid?

Fysieke en digitale beschermingsmaatregelen

De volgende vragen gaan over beschermingsmaatregelen gericht op fysieke en digitale toegang binnen uw instelling.

[31] 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.

25. Kunt u het huidige kennisveiligheidsbeleid van uw instelling met betrekking tot fysieke en digitale beschermingsmaatregelen scoren aan de hand van onderstaande rubric?

	Geen beleid	Beleid is nu in ontwikkeling	Beleid is vastgesteld en de uitvoering is aantoonbaar	Er is een verbetercyclus aanwezig en gedocumenteerd	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Fysieke en digitale beschermings-maatregelen					

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 instelling om met buitenlandse reisdelegaties die ruimtes met een restrictief toegangsbeleid op uw instelling bezoeken?
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 instelling met zeer sensitieve gegevens werkt: werkt uw instelling met rubricering van documenten (zoals ‘vertrouwelijk’ of ‘geheim’)?
28. Wat is de samenhang tussen cyberveiligheidsbeleid en het kennisveiligheidsbeleid op uw instelling?
29. Heeft u verder nog opmerkingen of een toelichting ten aanzien van fysieke en digitale beschermingsmaatregelen?

Internationale partnerschappen

Hieronder vragen we in welke mate uw instelling aan verschillende beleidsmaatregelen ten aanzien van internationale partnerschappen invulling geeft en wat daarbij de overwegingen zijn.

30. Kunt u het huidige kennisveiligheidsbeleid van uw instelling met betrekking tot internationale partnerschappen scoren aan de hand van onderstaande rubric?

	Geen beleid	Beleid is nu in ontwikkeling	Beleid is vastgesteld en de uitvoering is aantoonbaar	Er is een verbetercyclus aanwezig en gedocumenteerd	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Internationale partnerschappen					

31. Is er op bestuursniveau een centraal en up-to-date overzicht van veiligheidsgevoelige partnerschappen en financiering?
    a) Hoe wordt dit overzicht actueel gehouden?
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?
33. Heeft uw instelling beleid om te voorkomen dat (instituten binnen) uw instelling in een situatie van ongewenste (financiële) afhankelijkheid van statelijke actoren kan worden gebracht?
    a) Zo ja, kunt dit toelichten? Hoe ziet dit beleid eruit?
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 instelling (automatisch) gealerteerd ruim voor het verlengmoment, zodat er voldoende tijd is om de afspraken kritisch tegen het licht te houden?
35. Heeft u verder nog opmerkingen of een toelichting ten aanzien van internationale partnerschappen?

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 instelling hier mee te maken heeft en mee omgaat.

36. Kunt u het huidige kennisveiligheidsbeleid van uw instelling met betrekking tot juridische kaders en gedragscodes scoren aan de hand van onderstaande rubric?

	Geen beleid	Beleid is nu in ontwikkeling	Beleid is vastgesteld en de uitvoering is aantoonbaar	Er is een verbetercyclus aanwezig en gedocumenteerd	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Juridische kaders en gedragscodes					

37. Hoe is compliance met EU-exportcontrole van *dual use*-technologie[32] geborgd binnen uw instelling?
    a) Hoe wordt binnen uw instelling bepaald of een technologie *dual use* is?
38. Hoe is compliance met niet-EU import- en exportregels geborgd? U kunt hierbij denken aan het in- en doorverkopen van Amerikaanse apparatuur.
39. Hoe is compliance met internationale en EU-sanctieregimes (bijvoorbeeld ten aanzien van Rusland of Iran) geborgd binnen uw instelling?
40. Hoe worden gedragscodes zoals het Kader Kennisveiligheid Universiteiten of de EU guidelines on Tackling R&I foreign interference, of andere gedragscodes, binnen uw instelling toegepast?
41. Heeft u verder nog opmerkingen of een toelichting ten aanzien van juridische kaders en gedragscodes?

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 kan worden geïmplementeerd in beleid om een beeld te krijgen hoe uw instelling hier invulling aan geeft.

42. Kunt u het huidige kennisveiligheidsbeleid van uw instelling met betrekking tot personeelsbeleid en gedragscodes scoren aan de hand van onderstaande rubric?

	Geen beleid	Beleid is nu in ontwikkeling	Beleid is vastgesteld en de uitvoering is aantoonbaar	Er is een verbetercyclus aanwezig en gedocumenteerd	Er is een instellingsbreed risico- en beheersprogramma waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus
Personeelsbeleid					

43. Is er op bestuursniveau een centraal en up-to-date overzicht van werknemers, gasten en gastwerknemers die een risico vormen op het gebied van kennisveiligheid? Waarom wel of niet?
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?
45. Hoe wordt er binnen uw instelling voor gezorgd dat HR-medewerkers veiligheidsbewust zijn (en in staat zijn om signalen die wijzen op een verhoogd risico op te pikken)?
46. In hoeverre voert uw instelling 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?

[32] 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.

47. Beschikt uw instelling over een specifiek beleid voor dienstreizen naar landen met een verhoogd risicoprofiel? Zo ja, kunt u dit kort beschrijven?
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?
49. Heeft u verder nog opmerkingen of een toelichting ten aanzien van personeelsbeleid?

Evaluatie en doorontwikkeling

Kennisveiligheid is een relatief nieuw onderwerp dat nog sterk in ontwikkeling is. Met onderstaande vragen kunt u dit perspectief voor uw instelling schetsen.

50. Wat zijn de belangrijkste dilemma's en vraagstukken voor uw instelling bij het vormgeven van kennisveiligheidsbeleid?
51. Heeft uw instelling voor het komend jaar voornemens voor het (door)ontwikkelen van kennisveiligheidsbeleid in uw instelling? Zo ja, welke voornemens zijn dat?
52. Wordt het beleid, procedures, en maatregelen op het gebied van kennisveiligheid binnen uw instelling geëvalueerd? Zo ja, gebeurt dit op structurele basis? Wie zijn hierbij betrokken?

Afsluiting

53. Zijn er onderdelen van uw kennisveiligheidsbeleid die hierboven niet aan bod zijn gekomen? Zo ja, dan kunt u deze hier kort noemen.
54. Als u opmerkingen over het onderzoek of suggesties om deze vragenlijst te verbeteren heeft, dan kunt u die hieronder kwijt:
    ….

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, 22 december 2023
In opdracht van het ministerie van OCW