Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek

Sectorbeeld Universiteiten

Johan Bokdam en 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

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 universiteiten. Later dit jaar volgt een sectorbeeld voor de hogescholen. Begin 2024 volgt een sectorbeeld voor de KNAW- en NWO-instituten.

Achtergrond, doel en aanpak
Dit sectorbeeld brengt in kaart waar universiteiten staan met de uitwerking van hun 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 universiteiten risicoanalyses hebben uitgevoerd.
Het onderzoek is uitgevoerd middels een begeleide zelfevaluatie onder 14 universiteiten, aangevuld met een kwalitatief verdiepend case study onderzoek bij drie universiteiten. 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.

Het overgrote deel van de universiteiten operationaliseert kennisveiligheid op dezelfde wijze als de Leidraad. Een aantal vindt de uitbreiding van nationale veiligheid naar het beschermen van de Nederlandse innovatiekracht ongewenst.
Het kennisveiligheidsbeleid is in de praktijk voornamelijk gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie. Dit onderwerp wordt als het meest prangend, maar ook het meest concreet, ervaren. Er is beperkter aandacht voor het signaleren van en acteren op heimelijke beïnvloeding en ethische kwesties.

Beleid in ontwikkeling
Vanaf 2022 is het kennisveiligheidsbeleid bij alle universiteiten in een stroomversnelling geraakt. Verschillende universiteiten en faculteiten waren al langer bezig met onderdelen hiervan, bijvoorbeeld als gevolg van sanctieregelingen of door discussies over internationale partnerschappen met landen waar grondrechten niet worden gerespecteerd.

Het belang van het thema kennisveiligheid wordt gedragen door alle universiteiten. In ieder geval een kern van betrokkenen heeft het probleem zich eigen gemaakt, bij een deel van de instellingen en faculteiten is het al ingedaald op alle niveaus in de organisatie.
In het algemeen stellen we vast dat universiteiten actief bezig zijn om de adviezen van de Leidraad vorm te geven en dat ze gehoor hebben gegeven aan het verzoek van de minister van OCW tot een risicoanalyse in 2022. Het organisatorisch beleggen van verantwoordelijkheden en het ontwikkelen van beleid is verder gevorderd dan het vastleggen en uitvoeren van beleid in processen. De universiteiten hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie tabel S.1). Daarbij zien we een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad:

- Beleid op fysieke en digitale bescherming is veelal vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid.
- Beleid op risicoanalyses en -management van internationale partnerschappen en de doorwerking van juridische kaders is bij een aantal universiteiten al vastgesteld, maar meestal nog in ontwikkeling.
- De doorvertaling van kennisveiligheid naar personeelsbeleid is bij vrijwel alle universiteiten in ontwikkeling.

Tabel S.1 Fase van ontwikkeling kennisveiligheidsbeleid universiteiten, naar onderdeel Leidraad (n=14).

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en in uitvoering	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig	Er is instellings-breed beleid met verbetercyclus
Risicoanalyse	0	9	1	3	1	0	0
Risicomanagement	0	9	2	2	1	0	0
Fysieke en digitale beschermings-maatregelen	0	2	3	7	0	0	1
Internationale partnerschappen	0	9	1	3	0	1	0
Juridische kaders	0	10	1	1	1	0	0
Personeelsbeleid	1	12	0	1	0	0	0

Risicoanalyses
De minister van OCW heeft in 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren. Bijna alle universiteiten (13 van de 14) hebben deze afgerond, meestal aan de hand van het UNL model. Eén universiteit is er nog mee bezig. Voor zes universiteiten was de risicoanalyse naar aanleiding van de oproep van de minister een eerste ervaring met het doen van een dergelijke risicoanalyse.

Ongeveer de helft van de universiteiten ziet dat het uitvoeren van deze risicoanalyse heeft bijgedragen aan het creëren van meer bewustzijn van kennisveiligheidsrisico's. Vier universiteiten hebben nieuwe risico's geïdentificeerd, zeven universiteiten hebben naar aanleiding van de uitkomsten van de risicoanalyse nieuwe maatregelen genomen of hun beleid op het gebied van kennisveiligheid aangepast. Naast de analyse op verzoek van de minister werken alle universiteiten aan het ontwikkelen of uitvoeren van beleid voor het identificeren van kennisveiligheidsrisico's. De meeste universiteiten hebben hun sensitieve kennisgebieden in kaart gebracht, en bij de helft van de universiteiten treden standaard-processen in werking bij een bepaald risiconiveau.

Risicomanagement en fysieke en digitale maatregelen
De organisatie voor het beheren van kennisveiligheidsrisico's heeft op alle universiteiten de aandacht en is in ontwikkeling of in uitvoering. Alle universiteiten hebben een bestuurlijk portefeuillehouder kennisveiligheid en bijna overal is een Adviesteam Kennisveiligheid met een brede samenstelling aan expertises. Dit team heeft zowel de rol als intern loket, als een beleidsvormende functie. Vaak wordt beleid of protocollen aan de hand van casuïstiek ontwikkeld. De waarde van een moreel beraad bij het omgaan met ethische kwesties op het gebied van kennisveiligheid wordt op verschillende universiteiten verkend.

Een essentieel onderdeel van de organisatie van kennisveiligheidsbeleid is het vergroten van het kennisveiligheidsbewustzijn onder het personeel. Onderzoekers als inhoudelijk experts zijn noodzakelijk voor het signaleren van kennisveiligheidsrisico's en worden meegenomen in het risicomanagement. De meeste universiteiten geven aan bewustwordingscampagnes te voeren, ook specifiek gericht op HR-medewerkers.

De meeste universiteiten hebben restrictief toegangsbeleid voor bepaalde ruimtes, zodat gevoelige ruimtes enkel toegankelijk zijn voor aangewezen personen. Ook hebben 10 van de 14 universiteiten restrictief toegangsbeleid voor digitale onderzoeksgegevens en documenten. Dit beleid is veelal ontwikkeld buiten de context van kennisveiligheid.

Internationale partnerschappen en juridische kaders
De meeste universiteiten geven aan dat het beleid rondom internationale partnerschappen in ontwikkeling is. Vijf universiteiten hebben een partneracceptatiebeleid, bij zes universiteiten is dit in ontwikkeling. Hierbij worden samenwerkingsprojecten beoordeeld op inhoudelijke en financiële aspecten en wordt beoordeeld welke kansen of risico's een samenwerkingspartner geeft. Het creëren van centrale overzichten van internationale partnerschappen is lastig doordat samenwerkingen decentraal (op het niveau van faculteiten) worden aangegaan en het niet altijd goed te bepalen is wie samenwerkingspartners zijn. Internationale consortia kunnen bestaan uit tientallen partners, en een Europees bedrijf kan een dochteronderneming zijn van een moederbedrijf uit een risicoland. Daarnaast hebben instellingsbesturen beperkt tot geen zicht op individuele samenwerkingen die wetenschappers aangaan zonder institutionele contracten.

Ook voor compliance met juridische kaders geldt dat dit in sterke mate afhankelijk is van individuele onderzoekers voor het signaleren van onder meer dual-use toepassingen van hun onderzoek. Onderzoekers zijn echter beperkt op de hoogte van de juridische kaders. Deze kennis bij elkaar brengen vraagt aandacht.

Personeelsbeleid
Op bijna alle universiteiten is de vertaling van kennisveiligheidsbeleid in personeelsbeleid en gedragscodes nog in ontwikkeling. Negen van de 14 universiteiten onderneemt activiteiten gericht op het vergroten van kennis en bewustzijn van kennisveiligheid, bij vier universiteiten is dit nog in ontwikkeling. Ook wordt of is op een deel van de instellingen kennisveiligheid onderdeel van brede trainingen rondom integer onderzoek voor nieuwe medewerkers.

Enkele universiteiten wegen veiligheidsrisico's mee bij (een deel van) de werving en selectie van nieuwe medewerkers. Ze zijn tegelijk zoekend, op welke manier en bij welke werving dat te doen. Daarbij is het

van belang dat dit niet leidt tot discriminatie en uitsluiting. Ook is het van belang dat sollicitatieprocedures geen vertraging oplopen.

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. Universiteiten zijn zich bewust van de risico's op heimelijke beïnvloeding, maar beleid hierop is nog beperkt aanwezig. Twee universiteiten hebben hiervoor beleid, bij zes universiteiten is het in ontwikkeling; zes andere universiteiten geven ten slotte aan hier geen beleid voor te ontwikkelen.

Dilemma's ten aanzien van het kennisveiligheidsbeleid

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

- Het kennisveiligheidsbeleid is in sterke mate gericht op **technologisch onderzoek**, met veel aandacht voor het voorkomen van ongewenste overdacht van sensitieve kennis en technologie. De relevantie en proportionaliteit van kennisveiligheidsbeleid is daarom geregeld lastig te bepalen en onderbouwen voor met name de brede universiteiten.
- Kennisveiligheidsbeleid vraagt om een **nieuwe balans** tussen **academische waarden en nationale veiligheid**. Wetenschappelijk onderzoek is sterk gericht op kennisdeling en internationale samenwerking en kent traditioneel weinig structuren om kennis juist te beschermen. De structuren, culturen en motivaties vanuit deze twee opvattingen botsen in de praktijk.
- Een belangrijke zorg is **het voorkomen van stigmatisering en discriminatie**, of een cultuur van uitsluiting op terreinen waar er geen duidelijke sancties of juridische kaders zijn. Abstract nationaal beleid vertaalt zich binnen de instellingen tot impact op het individuele niveau van veelbelovende sollicitanten en gewaardeerde collega's.
- Binnen universiteiten speelt een **kennisdilemma.** Onderzoekers zijn zelf het beste in staat in te schatten of specifieke samenwerkingen veiligheidsrisico's met zich meebrengen. Zij hebben echter weinig kennis van formele exportregels of sanctiewetgeving. De mensen binnen de universiteit die dit wel hebben, missen vaak de inhoudelijke kennis om voor een specifiek samenwerkingsproject inhoudelijk te bepalen of er kennisveiligheidsrisico's aan zijn verbonden.
- Het kennisveiligheidsbeleid, de Leidraad en de voorbereidingen voor wetgeving rondom screening leiden tot discussies over de juiste **afbakening van verantwoordelijkheden** tussen universiteiten en de nationale overheid. De Nederlandse overheid legt op dit moment veel verantwoordelijkheid bij universiteiten. Dit vinden de meeste betrokkenen een goed uitgangspunt, omdat het een inhoudelijke genuanceerde afweging mogelijk maakt. Wel vragen universiteiten om middelen en informatiebronnen die hen in staat stellen om die verantwoordelijkheid te nemen. Ook wordt de vraag opgeworpen wat een universiteit van zichzelf en een overheid van een universiteit mag verwachten. Veel betrokkenen geven aan dat ze niet naïef willen zijn, maar ook reëel zijn over wat een universiteit vermag tegenover gerichte inspanningen van statelijke actoren om bepaalde kennis te verzamelen.
- Tot slot is er vanuit het belang van een **internationaal gelijk speelveld** (en het voorkomen van een internationaal waterbedeffect) behoefte aan consistent en afgestemd nationaal en Europees beleid.

Aandachtpunten

Naast dilemma's komen uit het sectorbeeld ook een aantal aandachtspunten voor het verdere beleid:

- **Conceptualisering van kennisveiligheid**. Instellingen die al verder zijn in hun beleidsontwikkeling, geven vaak een eigen invulling aan wat zij wel en niet onder kennisveiligheid (willen) verstaan.

Daarnaast wordt in de praktijk op verschillende manieren invulling gegeven aan begrippen als samenwerking, partnerschappen, kroonjuwelen en dual-use toepassingen, wat invloed heeft op het analyseren en mitigeren van risico's. Het zou nuttig zijn om hier als overheid en sector gezamenlijk verder aan zowel conceptualisering als definiëring te werken, en dit te verwerken in een volgende editie van de Nationale Leidraad Kennisveiligheid.

- **Verantwoordelijkheid**. De overheid legt op dit moment veel verantwoordelijkheid bij universiteiten. Dit vinden de meeste betrokkenen een goed uitgangspunt, omdat het een inhoudelijke genuanceerde afweging mogelijk maakt. Wel vragen universiteiten om duidelijke (afwegings)kaders, middelen en informatiebronnen die hen in staat stellen om die verantwoordelijkheid te nemen. Tegelijk erkennen gesprekspartners dat het moeilijk zal zijn om deze helderheid te geven. Bestaande kaders en lijsten worden ofwel te generiek bevonden, ofwel te lang en onoverzichtelijk.
- **Blijvende dialoog en onderling vertrouwen**. Een blijvende dialoog en onderling vertrouwen tussen de overheid en de wo-sector zijn van belang. Er is waardering voor het Loket Kennisveiligheid en voor de verbindende rol van het ministerie van OCW. Tegelijkertijd zijn er zorgen dat beleidsontwikkelingen en verzoeken vanuit de overheid elkaar te snel opvolgen, waardoor implementatie of doorwerking in de instellingen minder nauwkeurig of genuanceerd vorm kan krijgen.

1 Inleiding

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 universiteiten. Later dit jaar volgt een sectorbeeld voor de hogescholen. Begin 2024 volgt 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,[1] 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.[2] In het spoeddebat kennisveiligheid was deze externe audit eerder aangekondigd in de Tweede Kamer.[3] 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,[4] 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.

Bovendien stellen we vast dat hier sprake is van een momentopname: de kern van het onderzoek is waar universiteiten en hogescholen medio 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 om een risicoanalyse[5] van kennisveiligheid uit te voeren of te actualiseren. Het onderzoek geeft op deze manier invulling aan de externe audit kennisveiligheid die de minister in de Tweede Kamer heeft aangekondigd. 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.

---

1 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

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

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

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

5 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 universiteiten. Daarbij 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. Het onderzoek levert een beeld op van waar de sector nu staat op het gebied van kennisveiligheidsbeleid.
Dit leidt tot de volgende centrale onderzoeksvraag:
Waar staan de universiteiten 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 codes).
4 Personeelsbeleid.

We volgen bovendien het advies van de AWTI voor een **lerende aanpak**.[6] 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 universiteiten zich geconfronteerd zien en eventuele *lessons learned* waar universiteiten van elkaar kunnen leren. Naast dit sectorbeeld ontvangen alle universiteiten daarom een individuele terugkoppeling die alleen wordt gedeeld met hen, 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 universiteiten een vragenlijst voorgelegd kregen die zij puntsgewijs dienden te beantwoorden. In het geval een vraag niet goed begrepen werd konden universiteiten contact opnemen met de onderzoekers.

6 AWTI (2022). Kennis in conflict. Veiligheid en vrijheid in balans.

Tabel 1.1 Onderzoeksopzet 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
Uitvoering zelfevaluatie door de instellingen	• Uitzetten vragenlijst en persoonlijk contact • Invullen vragenlijst door instellingen • Nazorggesprek en duiding	Februari Februari tot en met april April
Kwalitatieve verdieping	• Selectie cases • Benadering, uitvoering en verslaglegging cases (3)	Mei Mei en juni
Analyse en rapportage	• Analyse vragenlijsten • Rapportage • Bespreken conceptrapport met klankbordgroep	Mei Juni Juli 2023

1.3.1 Voorbereiding

De voorbereidingsfase 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 drietal kennisinstellingen. Zij hebben in gesprek met een onderzoeker de vragenlijst doorgelopen en van commentaar voorzien.

De vragenlijst is vervolgens besproken met de **klankbordgroep** die voor dit onderzoek is ingesteld. Daarin 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 bestaat uit vertegenwoordigers van UNL, VH, NWO, KNAW, de Universiteit Twente, Tilburg University, UMC Utrecht en UMC Groningen.

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 is opgenomen in bijlage 1. De samenstelling van de klankbordgroep staat in bijlage 2.

1.3.2 Uitvoering zelfevaluatie

De goedgekeurde vragenlijst voor de zelfevaluatie voor het sectorbeeld universiteiten is in februari 2023 uitgezet onder contactpersonen van de 14 betrokken universiteiten 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 universiteiten. 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) en 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 achtergrondkenmerken (één technische universiteit, één brede universiteit met een UMC, een brede universiteit algemeen) en spreiding op basis van de zelfevaluatie naar inhoudelijk relevante praktijken op omgang met verschillende type risico's.
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 faculteiten (waaronder decanen en onderzoeksleiders) en HR. In totaal zijn 21 gesprekken gevoerd.

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. Gesloten vragen (ja/nee) zijn kwantitatief geanalyseerd. De resultaten uit die analyse en de analyse van de caseverslagen zijn integraal samengebracht in dit sectorbeeld voor de universiteiten.

2 Kennisveiligheidsbeleid

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

2.1 Afbakening kennisveiligheid

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 gegevens in de kamerbrief van november 2020.[7] In dit rapport schrijven we in het kort over **sensitieve kennis en technologie**, **heimelijke beïnvloeding** en **ethische kwesties** als de onderwerpen van kennisveiligheid.

Het overgrote deel van de universiteiten geeft aan dat zij het beleidsthema op dezelfde wijze afbakenen. Hierbij geven meerdere universiteiten expliciet aan de definitie van de Leidraad (vier universiteiten) of de brief van OCW (drie universiteiten) te volgen.

Een aantal andere universiteiten is vertrokken vanuit deze afbakening, maar heeft deze aangepast aan de eigen visie. Van deze groep geven meerdere universiteiten aan dat zij het beschermen van de Nederlandse innovatiekracht niet zien als een kerntaak van universiteiten en dit daarom hebben weggelaten uit hun definitie. In een gesprek bij een universiteit wordt aangegeven dat de koppeling met de Nederlandse innovatiekracht (en het Nederlandse verdienvermogen) een risico is voor het draagvlak voor kennisveiligheidsbeleid. Wetenschappers begrijpen maar al te goed dat zij met hun onderzoek de nationale veiligheid niet willen schaden, maar vinden het niet wenselijk om zelf de kennisontwikkeling en innovatiekracht te borgen voor het Nederlands bedrijfsleven in concurrentie met het niet-Europees bedrijfsleven.

Twee universiteiten geven verder aan dat zij heimelijke beïnvloeding breder zien dan statelijke actoren, maar hier ook niet-statelijke actoren in meenemen (bijvoorbeeld bedrijven, politici of non-governmental organisations). Ten slotte laten vier universiteiten ethische kwesties buiten de afbakening van kennisveiligheid, omdat dit onderwerp los van het kennisveiligheidsbeleid is belegd bij de commissies voor de ethische beoordeling van onderzoek en onderzoeksvoorstellen.

---

[7] kamerbrief over maatregelen kennisveiligheid hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl

In de beantwoording van de zelfevaluatie en de gesprekken bij universiteiten valt ons op dat het kennisveiligheidsbeleid voornamelijk is gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie (en minder op heimelijke beïnvloeding en ethische kwesties). Dit onderwerp wordt als het meest prangend, maar ook het meest concreet, ervaren.

Bij heimelijke beïnvloeding en ethische kwesties verwijzen veel betrokkenen ook naar de gedragscode wetenschappelijke integriteit.[8] Kennisveiligheid introduceert een nieuwe balans waarin keuzes moeten worden gemaakt tussen academische kernwaarden en overwegingen over nationale veiligheid. Universiteiten onderstrepen het belang van internationale samenwerking, autonomie en academische vrijheid als randvoorwaarden voor excellent onderzoek. Universiteiten zijn van oudsher gericht op kennisdeling, zowel binnen als buiten de instelling en hebben traditioneel geen structuren om kennis juist te beschermen. Ook geven enkele instellingen aan onduidelijkheid te ervaren hoe het kennisveiligheidsbeleid zich dient te verhouden tot het overheidsbeleid naar meer *open science*, wat juist moet leiden tot meer toegankelijkheid van wetenschappelijke kennis.

2.2 Ontwikkeling van kennisveiligheidsbeleid

Hoewel kennisveiligheid als beleidsthema relatief recent is, geven verschillende universiteiten aan al langer bezig te zijn met onderdelen die (nu) onder dit thema worden geschaard. Zo gelden verschillende sanctieregelingen al voor lange tijd (bijv. de sanctieregelingen voor Noord-Korea en Iran sinds 2007). Sinds 2019 heeft de Rijksoverheid een interdepartementaal Taskforce ongewenste kennisoverdracht bestaande uit medewerkers van de ministeries van Buitenlandse Zaken (BZ), Justitie & Veiligheid (J&V) en Onderwijs, Cultuur en Wetenschap (OCW), naar aanleiding van kwesties die speelden in 2018.[9] Verschillende universiteiten geven dan ook aan sinds 2018 actief beleid te ontwikkelen op veiligheidsrisicomanagement en borging van compliance met sanctiewetgeving en export controle. De Nationale Leidraad van januari 2022 is dan ook tot stand gekomen dankzij bijdragen van en discussies onder universiteiten (alsook anderen, waaronder KNAW, NFU, VH, TO2-federatie en NWO).

In 2022 is het kennisveiligheidsbeleid van universiteiten in een stroomversnelling geraakt. Informele werkgroepen en ontwikkelingen zijn in 2022 veelal geformaliseerd in adviesteams en werving van aangewezen beleidsadviseurs, coördinatoren of programma-/projectmanagers. Dit geldt voor acht universiteiten. Eén universiteit geeft aan dat er nog geen behoefte is aan een instellingsbreed programma, maar dat zij verkennen of op facultair niveau behoefte is aan kennisveiligheidsbeleid.

Alle universiteiten geven aan dat het kennisveiligheidsbeleid nog volop in ontwikkeling is. Dit zijn meerjarenprogramma's waarin het bewustzijn van kennisveiligheidsoverwegingen op de werkvloer wordt vergroot, verantwoordelijkheden voor het afwegen van risico's en kansen worden aangescherpt en verder in kaart wordt gebracht welke kennisgebieden en afdelingen (extra) aandacht verdienen in het kader van kennisveiligheid. Een aantal universiteiten geeft aan dat zij ook verwachten dat aanpassingen in landelijke wetgeving de komende jaren zullen leiden tot doorontwikkeling van het

8 KNAW, NFU, NWO, TO2, VH, UNL (2018) Nederlandse gedragscode wetenschappelijke integriteit

9 Kamerstuk 30821, nr. 70 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

kennisveiligheidsbeleid. Een belangrijke onderwerp waar universiteiten afhankelijk zijn van wetgeving is onder meer het aangekondigde Wetsvoorstel Screening Kennisveiligheid.[10]
De universiteiten hebben hun fase van beleidsontwikkeling zelf gescoord in een rubric (zie Tabel 2.1).[11]
Daarbij zien we een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad:

- Beleid op fysieke en digitale bescherming is veelal vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid
- Beleid op risicoanalyses en -management van internationale partnerschappen en de doorwerking van juridische kaders is bij een aantal universiteiten al vastgesteld, maar meestal nog in ontwikkeling
- De doorvertaling van kennisveiligheid naar personeelsbeleid is bij vrijwel alle universiteiten in ontwikkeling

Tabel 2.1 Fase van ontwikkeling kennisveiligheidsbeleid universiteiten, naar onderdeel Leidraad (n=14[12]).

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en in uitvoering	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig	Er is instellings-breed beleid met verbetercyclus
Risicoanalyse	0	9	1	3	1	0	0
Risicomanagement	0	9	2	2	1	0	0
Fysieke en digitale beschermings-maatregelen	0	2	3	7	0	0	1
Internationale partnerschappen	0	9	1	3	0	1	0
Juridische kaders	0	10	1	1	1	0	0
Personeelsbeleid	1	12	0	1	0	0	0

Een aantal universiteiten scoort zichzelf tussen twee niveaus of scoort beleid deels op één niveau en deels op het volgende. Dit heeft geleid tot (extra) kolommen “Beleid is deels in ontwikkeling, deels vastgesteld en in uitvoering” en “Beleid kent deels een verbetercyclus”. Het laatste niveau van de rubric is dat er een instellingsbreed risico- en beheersprogramma is waarin beleid geïmplementeerd en gedocumenteerd wordt in een verbetercyclus.

Doordat het beleid op instellingen nog sterk in ontwikkeling is, geven 13 (van de 14) universiteiten aan nog geen structurele evaluaties van het beleid uit te voeren. Enkele instellingen benoemen dat zij bij de implementatie van beleid en de bespreking van casuïstiek ook het beleid beschouwen en hierbij eventueel aanpassingen doorvoeren. Eén universiteit evalueert het kennisveiligheidsbeleid jaarlijks en voert ook performance reviews en audits uit over meerdere jaren. Vijf universiteiten geven aan dat zij van plan zijn om in de toekomst het beleid te evalueren of dat zij in de ontwikkeling van het kennisveiligheidsbeleid ook het evaluatiebeleid daarvan ontwikkelen.

---

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

11 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.

12 Bij fysieke en digitale beschermingsmaatregelen en juridische kaders hebben niet alle universiteiten zichzelf gescoord.

3 Risicoanalyses

De minister van OCW heeft op 4 april 2022 de kennisinstellingen gevraagd een risicoanalyse van kennisveiligheid uit te voeren of te actualiseren.[13] 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 het onderzoek, (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 eerst dit verzoek en op welke manier instellingen hieraan invulling hebben gegeven (3.1). In paragraaf 3.2 gaan we in op de risicoanalyse als onderdeel van het kennisveiligheidsbeleid van universiteiten. Vervolgens behandelen we de dilemma's en aandachtpunten in paragraaf 3.3. In paragraaf 3.4 beschrijven we de lessons learned van de universiteiten.

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.[14] 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. Risicovolle samenwerkingen en financieringsbronnen verdienen hierbij bijzondere aandacht. De minister omschrijft dat het hierbij van belang is dat er op bestuursniveau een actueel en volledig overzicht bestaat, en dat overeenkomsten waarin academische kernwaarden onvoldoende zijn geborgd of die grote risico's met zich meebrengen dienen te worden herzien of ontbonden.

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 er 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 universiteiten

Verreweg het grootste deel (13 van de 14) van de universiteiten heeft naar aanleiding van de oproep van de minister een risicoanalyse uitgevoerd. Bij één universiteit is deze analyse nog in ontwikkeling. Deze instelling is bezig met het uitvoeren van een risicoanalyse maar volgt hierbij haar eigen

---

13 Afschrift brief aan kennisinstellingen Nationale Leidraad Kennisveiligheid | Brief | Rijksoverheid.nl

14 Zie Home | Loket Kennisveiligheid

beleidscyclus, omdat het doen van een risicoanalyse voor de gehele instelling veel tijd kost. De instelling ziet dit als een meerjarige opgave. De meeste universiteiten (13 van de 14) hebben gebruik gemaakt of maken gebruik van een bestaand model, bijvoorbeeld het model voor risicoanalyse voor kennisveiligheid van UNL[15] of de Kwetsbaarheidsanalyse Spionage van de AIVD[16]. Vooral het model van UNL wordt in de zelfevaluaties vaak genoemd (tenminste door tien universiteiten). In dit model wordt het inschatten van risico's beschreven aan de hand van drie onderwerpen (conform de Leidraad):

1. Kennisgebieden met een verhoogd risico
2. Landen met een verhoogd risico
3. Samenwerkingspartners, opdrachtgevers en financiers

Naast het gebruik van deze twee modellen, geven twee universiteiten aan hulp te hebben ingeschakeld van het Loket Kennisveiligheid of contact te hebben gehad met hun contactpersoon bij de Veiligheidsdiensten.

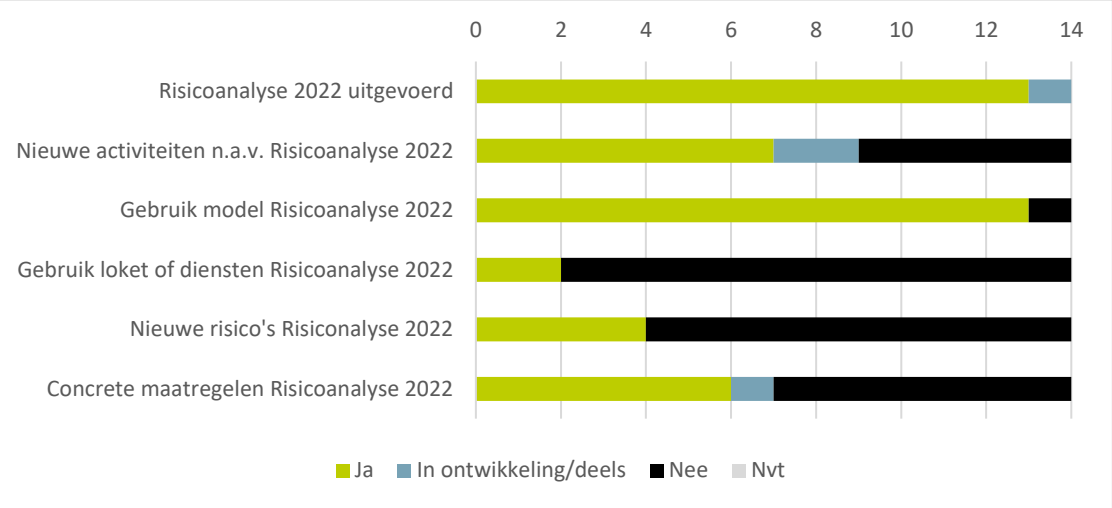
Het **uitvoeren van de risicoanalyse** naar aanleiding van de oproep van de minister heeft voor zeven universiteiten geleid tot nieuwe of andere activiteiten in vergelijking met eventuele risicoanalyses die binnen de instelling al werden uitgevoerd; twee universiteiten zijn hier nog mee bezig. Universiteiten zijn bijvoorbeeld extra data-analyses uit gaan voeren, of geven extra aandacht aan bewustzijn van kennisveiligheid bij medewerkers of de geldende wet- en regelgeving.
Bij vijf universiteiten heeft de oproep voor de risicoanalyse niet geleid tot het aanpassen of toevoegen van activiteiten op het gebied van risicoanalyses voor kennisveiligheid. Voor hen was de gevraagde risicoanalyse een bevestiging van de ingezette koers, die zij verder voortzetten.
Zes universiteiten geven aan dat dit de eerste keer was dat ze op deze schaal een risicoanalyse uitvoerden, zij deden dit bijvoorbeeld eerder uitsluitend op decentraal niveau. Over het algemeen geven de universiteiten aan dat een eerste analyse op deze schaal - naar aanleiding van de oproep van de minister - niet betekent dat er voorheen geen acties waren op het gebied van kennisveiligheid en risicoanalyse. Er was bijvoorbeeld al wel bewustzijn binnen de instellingen van het belang van kennisveiligheid of er waren al gesprekken over. Sommige universiteiten hadden al een kleinere verkennende analyse uitgevoerd. Voor het grootste deel van de andere universiteiten was het uitvoeren van een risicoanalyse op deze schaal dus niet (geheel) nieuw.

De **uitkomsten van de risicoanalyse** bieden in wisselende mate nieuwe inzichten voor universiteiten. Door vier universiteiten is bijvoorbeeld aangegeven dat zij nieuwe risico's hebben geïdentificeerd, en zeven universiteiten hebben naar aanleiding van de uitkomsten van de risicoanalyse nieuwe maatregelen genomen of hun beleid op het gebied van kennisveiligheid aangepast. Universiteiten letten bijvoorbeeld scherper op bestaande samenwerkingen, waar ook heimelijk beïnvloeding uit kan voortkomen. Nieuwe risico's worden vooral gezien op het gebied van samenwerkingen of in (combinaties van) specifieke typen onderzoek (denk bijvoorbeeld aan het gebruiken van datasets met gevoelige gegevens in disciplines waar nog beperkt aandacht was voor kennisveiligheid), of risico's die voortkomen uit de combinaties tussen risicovolle landen en onderzoeksgebieden. Aanpassingen aan het beleid of genomen maatregelen komen bijvoorbeeld voort uit de noodzaak van het creëren van meer bewustzijn binnen de instelling met betrekking tot kennisveiligheid, maar door ongeveer de helft van de

[15] Naar aanleiding van de oproep van de minister heeft UNL een model ontwikkeld om universiteiten te faciliteren de risicoanalyse op systematische wijze uit te kunnen voeren. Dit model is ontwikkeld voor intern gebruik. Universiteiten van Nederland (2022). Model Risicoanalyse Kennisveiligheid.

[16] Algemene Inlichtingen en Veiligheidsdienst (2010). Kwetsbaarheidsanalyse Spionage.

universiteiten wordt ook gerapporteerd dat het uitvoeren van de risicoanalyse zelf bijgedragen heeft aan het creëren van meer bewustzijn. Voor sommige universiteiten bevestigde de risicoanalyse dat zij zich op de juiste vooropgezette route begeven.
Voor een overzicht van de antwoorden van universiteiten, zie Figuur 3.1.



Figuur 3.1 Overzicht activiteiten op risicoanalyses

3.2 Risicoanalyse als onderdeel van het kennisveiligheidsbeleid van universiteiten

Alle universiteiten zijn actief in het ontwikkelen of uitvoeren van beleid ten aanzien van het (continu) inschatten van risico's. Het merendeel van de universiteiten (9 van de 14) geeft aan dat het beleid nog in ontwikkeling is. Bij vier universiteiten is het beleid (bijna) vastgesteld en is de uitvoering aantoonbaar, en één universiteit geeft aan dat er ook al een verbetercyclus aanwezig is.

Het uitvoeren van de risicoanalyse naar aanleiding van de oproep van de minister was voor zes universiteiten een eerste ervaring met het doen van een dergelijke risicoanalyse. Andere universiteiten deden dit al op centraal en decentraal niveau. Enkele universiteiten geven expliciet aan dat zij risicoanalyses vooral doen als het gaat om nieuwe samenwerkingen of dat zij juist meer de focus hebben gelegd op bestaande samenwerkingen.

De risicoanalyses van de universiteiten 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. Hierbij valt op dat instellingen in de meeste gevallen er niet voor kiezen om een eigen lijst van sensitieve kennisgebieden te hanteren, maar gebruik te maken van bestaande lijsten. Ook valt op dat universiteiten maar beperkt 'kroonjuwelen' in kaart brengen. Dit zijn de gebieden waarop er risico's verbonden zijn aan kennisoverdracht en waar de instelling internationaal toonaangevend is. In de toelichtingen wordt aangegeven dat in de risicoanalyses voornamelijk wordt gekeken naar sensitieve kennisgebieden en er nog geen wens is geweest om een extra analyse uit te voeren naar een internationale ranking op deze sensitieve kennisgebieden.

Tabel 3.1. Toepassingen van risicoanalyses onder universiteiten

	Uitgevoerd	In ontwikkeling	Niet van toepassing	Opmerkingen
Identificatie sensitieve kennisgebieden	9	4	1	Alle (4) technische universiteiten hebben dit uitgevoerd.
Eigen lijst sensitieve kennisgebieden	3	3	8	
Identificatie kroonjuwelen	5	4	5	
Standaard-processen	7	3	4	Drie van de vier technische universiteiten hebben dit uitgevoerd, één is hiermee bezig.

Risicoanalyses vinden voornamelijk uitvoering via interne gesprekken tussen onderzoekers, bestuurders en medewerkers met kennis op het gebied van kennisveiligheid, vaak aan de hand van algemene richtlijnen die zich bijvoorbeeld richten op specifieke landen. Hierbij wordt voornamelijk gewerkt vanuit casuïstiek. Enkele universiteiten hebben ook een werkgroep of adviesgroep hiervoor ingericht. Veel universiteiten maken bovendien veelvuldig gebruik van openbare bronnen.[17]

3.3 Dilemma's en aandachtpunten

Universiteiten geven verschillende dilemma's en aandachtspunten mee op het gebied van risicoanalyse(s).

Universiteiten geven aan dat het werken met bronnen (zoals de sanctielijst) een laagdrempelige manier is om risico's van samenwerkingen met landen of personen in te schatten. Hierbij benadrukken zij wel dat het van belang is dat ze ervanuit kunnen gaan dat de bronnen actueel zijn. Tools voor risicoanalyses lijken vooral gericht op technologieën, waardoor universiteiten zelf moeten bedenken welke andere sensitieve kennisgebieden zij hebben en hoe zij hierop risico's kunnen inschatten.

Ook geven enkele universiteiten aan dat zij willen voorkomen dat het risicovolle imago dat nu gekoppeld wordt aan bepaalde landen (zoals bijvoorbeeld China, Rusland of Iran) ervoor zorgt dat al het onderzoek (ook op niet-risicovolle kennisgebieden) met onderzoekers of instellingen uit dergelijke landen onmogelijk wordt, of dat alle onderzoekers uit die landen zich buitengesloten gaan voelen.

Universiteiten zoeken tenslotte naar systemen die zo efficiënt mogelijk zijn: onderzoekers moeten zoveel mogelijk ontlast en gefaciliteerd worden om hun onderzoek goed uit te kunnen voeren. Daarom willen zij niet dat dergelijke risicoanalyses te veel tijd en inspanning van de onderzoekers vragen. Tegelijkertijd is de expertise van de onderzoekers essentieel om een inschatting te maken van de risico's.

[17] Voorbeelden van bronnen die gebruikt worden zijn de sanctielijsten van de EU en de VN, de China Defence Universities Tracker van ASPI, nationale en internationale exportregels (waaronder Europese en Nederlandse richtlijnen en regelgeving voor Dual Use/strategische goederen) en de lijst met Key Enabling Technologies van NWO.

3.4 Lessons learned

Uit de risicoanalyses komt een aantal geleerde lessen naar voren. Allereerst blijkt dat de verantwoordelijkheid voor kennisveiligheid bij veel universiteiten primair bij (de onderzoekers binnen) de vakgroepen zelf ligt, omdat risico's en bijbehorende acties kunnen verschillen per vakgroep. Hoewel de risicoanalyse naar aanleiding van de oproep van de minister vooral vanuit het centrale bestuur en in samenwerking met faculteiten en vakgroepen is uitgevoerd (top-down), lijkt een groot deel van de identificatie van risico's te gebeuren door onderzoekers die een signaal afgeven richting het instellingsbestuur als zij een risico vermoeden (bottom-up). In toenemende mate zijn er centrale werkgroepen actief binnen universiteiten, en worden er centrale adviescommissies of medewerkers aangesteld (zie ook hoofdstuk 4). Dit helpt bij het uitzetten van de risicoanalyse, en zorgt er tevens voor dat met behulp van de risicoanalyse een eenduidig overzicht gegeven kan worden op het gebied van kennisveiligheid.

Meerdere universiteiten hebben een beslisboom die in werking treedt als (onderzoekers in) de vakgroepen risico's signaleren. Hierdoor blijven de risico's overzichtelijk en is het voor medewerkers duidelijk waar zij hulp kunnen krijgen en waar het mandaat ligt om een besluit te nemen. Als een universiteit vervolgens zelf niet op een goede manier de risico's kan beoordelen, wordt advies gevraagd bij het loket kennisveiligheid of een contactpersoon van de veiligheidsdiensten.

Bij het uitvoeren van de risicoanalyse is vaak gebruik gemaakt van het model van UNL. Meerdere universiteiten geven aan dat zij dit model eerst intern besproken hebben en vervolgens aangepast aan de lokale context. De analyse is vervolgens veelal per faculteit uitgezet.

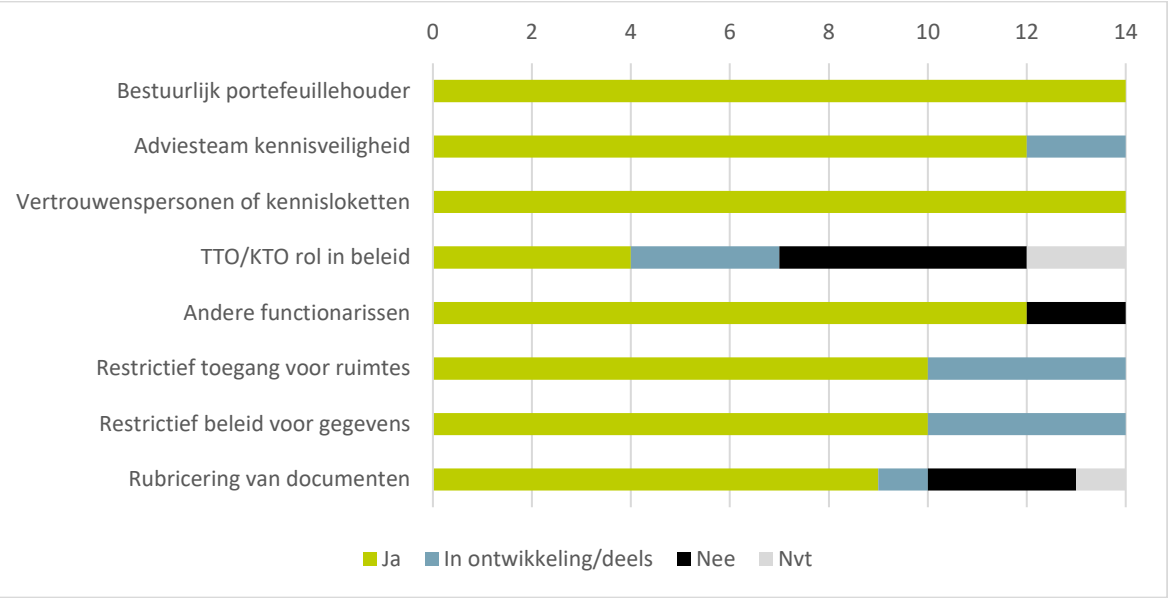
4 Risicomanagement en fysieke en digitale maatregelen

In dit hoofdstuk beschrijven we hoe universiteiten 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. Universiteiten zijn veelal decentrale organisaties, met een centraal onderdeel en autonome faculteiten. 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 geleerde lessen 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. Voor een overzicht van de activiteiten ten aanzien van risicomanagement aan universiteiten, zie Figuur 4.1.

Figuur 4.1 Overzicht activiteiten risicomanagement



Het risicomanagement van kennisveiligheid heeft op alle universiteiten de aandacht. Negen universiteiten geven aan dat dit beleid nu in ontwikkeling is, de overige 5 universiteiten geven aan dat dit beleid (bijna of helemaal) is vastgesteld en aantoonbaar in uitvoering is. Een enkele universiteit geeft aan al bezig te zijn met een verbetercyclus van bestaand beleid of dit beleid al instellingsbreed in risico- en beheersprogramma's te hebben opgenomen.

Alle universiteiten hebben een **bestuurlijk portefeuillehouder** kennisveiligheid aangewezen, meestal de voorzitter van het College van Bestuur. De rol van deze portefeuillehouder verschilt per universiteit, deels afhankelijk van de mate waarin het kennisveiligheidsbeleid is gevorderd. Bij de universiteiten waar het risicomanagement stevig is ingebed in de (verschillende lagen van de) organisatie en het adviesteam

sterk gepositioneerd is, kan de portefeuillehouder een grotere afstand nemen van de specifieke casuïstiek en zich vooral op strategisch niveau bezig houden met kennisveiligheid. Bij enkele universiteiten zien we dat de portefeuillehouder inhoudelijk nog (relatief) intensief betrokken is en actief onderdeel is van de escalatieladder van risicomanagement.

De Universitaire Medische Centra (UMC's) zijn in dit onderzoek meegenomen als onderdeel van de universiteit. In de praktijk lijkt de samenwerking op kennisveiligheid grotendeels te verlopen zoals die met andere faculteiten. UMC's zijn doorgaans wel veel groter dan andere faculteiten. Ook kennen ze in tegenstelling tot andere faculteiten een juridisch zelfstandige positie, met een eigen Raad van Bestuur, wat de bestuurlijke afstemming complexer maakt. Daarom worden ze door het ministerie van OCW dan ook geregeld formeel apart benaderd.

4.1.1 Organisatieonderdelen betrokken bij kennisveiligheid

Het overgrote deel van de universiteiten heeft op centraal niveau een **Adviesteam Kennisveiligheid** aangesteld. Op twee universiteiten is een soortgelijk team nog in oprichting. Het adviesteam bestaat vaak uit een kleine kern (tot 6 of 7 leden) met een schil daaromheen van experts en adviseurs die op ad hoc basis beschikbaar zijn voor specifieke casussen. De exacte samenstelling van het adviesteam varieert tussen universiteiten. Het kernteam bestaat vaak uit een programmamanager Kennisveiligheid, coördinator Integrale Veiligheid, de Chief Information Security Officer en overige beleidsmedewerkers kennisveiligheid. 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 universiteiten. Bij diverse universiteiten is dit een apart team met een specifiek mandaat, bij andere universiteiten is kennisveiligheid ondergebracht bij een programma of afdeling integrale veiligheid.

Het adviesteam is primair verantwoordelijk voor de ontwikkeling van het kennisveiligheidsbeleid en is veelal het aanspreekpunt voor kennisveiligheidsvraagstukken vanuit faculteiten. Zo is het adviesteam een belangrijke spil wanneer er twijfels zijn omtrent internationale partnerschappen of personeelswerving (zie hoofdstukken 5 en 6). Wanneer het adviesteam de vraag niet zelfstandig kan beantwoorden, legt zij de vraag bij het Loket Kennisveiligheid.

Het verkrijgen van beleidsmatige afstemming tussen het instellingsbrede kennisveiligheidsbeleid en de faculteiten is bij de meeste universiteiten belegd in bestaande overleggen, zoals het overleg tussen de decanen van een universiteit. Hierbij wordt de mate van afstemming tussen centraal en decentraal per faculteit bepaald aan de hand van kennisveiligheidsrisico's. Zo is er meer afstemming tussen het adviesteam en de faculteiten met een verhoogd kennisveiligheidsrisico of wordt in deze faculteiten een aanspreekpunt van het adviesteam gepositioneerd. Zo wordt bijv. binnen brede universiteiten meer aandacht besteed aan de technische faculteiten dan aan de geesteswetenschappelijke faculteiten.

Op alle universiteiten 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.

De **technology/knowledge transfer offices**, verantwoordelijk voor toepassing en valorisatie van kennis, worden maar beperkt meegenomen in het kennisveiligheidsbeleid. In de meeste universiteiten zijn ze geen onderdeel van de ontwikkeling van het kennisveiligheidsbeleid, in een aantal gevallen worden ze op de hoogte gehouden van de ontwikkeling van beleid. De voorname reden is dat de TTO's/KTO's aan

de achterkant van onderzoek zijn gepositioneerd, als het onderzoek is afgerond en valorisatiepotentieel heeft. Het kennisveiligheidsbeleid is echter primair gericht op de voorkant van het onderzoek, als een samenwerking wordt opgezet of personeel wordt geworven.

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 universiteiten aan dat ethische beoordeling reeds is georganiseerd, onafhankelijk van het kennisveiligheidsbeleid. Meerdere universiteiten laten ethische kwesties dan ook buiten hun afbakening van kennisveiligheid, zie eerder hoofdstuk 2.

Ten slotte geven enkele universiteiten aan een **moreel beraad** te ontwikkelen of al in te zetten voor het bespreken van kennisveiligheidsvraagstukken. In een moreel beraad bespreken beleidsmedewerkers samen met onderzoekers casuïstiek. Zo heeft bijvoorbeeld de TU Delft een pilot gedaan van een dergelijk moreel beraad aan de faculteit Elektrotechniek, Wiskunde en Informatica en na positieve evaluatie besloten dit voort te zetten.[18]

4.1.2 Ontwikkelen van bewustzijn van kennisveiligheid

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

De meeste universiteiten (9 van de 14) geven aan **bewustwordingscampagnes** te voeren rondom kennisveiligheid. Door middel van presentaties, nieuwsbrieven, workshops, kennislokketten en websites brengen of houden zij het personeel op de hoogte. Bewustwordingscampagnes zijn gericht op een breed scala aan medewerkers: van wetenschappelijk personeel, tot managers en HR-personeel dat betrokken is bij de werving en selectie van nieuwe medewerkers. Twee universiteiten geven aan dat de coördinator kennisveiligheid of (andere leden van) het adviesteam een rondgang doet langs overleggen om het thema op de agenda te zetten en te houden. Bij vier universiteiten worden bewustwordingscampagnes op dit moment deels uitgevoerd – bijvoorbeeld alleen binnen faculteiten met een verhoogd risicoprofiel – of is men nog bezig met de ontwikkeling van bewustwordingscampagnes.

Vijf universiteiten geven aan dat binnen hun instelling nog geen procedures zijn rondom het kennisveiligheidsbewust maken van **HR-medewerkers** (d.w.z. hen in staat stellen om kennisveiligheidsrisico's te signaleren) of dat het beleid hieromtrent nog in ontwikkeling is. Zij onderzoeken nog welke middelen passend zijn om HR-medewerkers in staat te stellen om hun veiligheidsbewustzijn te vergroten. De overige universiteiten geven aan specifiek het HR-personeel bewust te maken van kennisveiligheidsrisico's door middel van het aanbieden van richtlijnen, checklists, bewustwordingstrainingen, voorlichtingscursussen, modules en presentaties rondom kennisveiligheid.

---

18 TU maakt informatie over kennisveiligheid intern toegankelijk (tudelft.nl)

Wanneer we specifiek kijken naar de mate waarin nieuwe medewerkers informatie en **training** krijgen om hen kennisveiligheidsbewust te maken, zien we grote verschillen tussen universiteiten. Vier universiteiten bieden trainingen en informatiemodules voor al het nieuwe personeel, of specifiek voor nieuwe PhD-kandidaten. Drie van deze universiteiten geven trainingen gerelateerd aan informatiebeveiliging en/of andere veiligheidsthema's als wetenschappelijke integriteit, sociale veiligheid en cyberveiligheid, maar (nog) geen trainingen specifiek gericht op kennisveiligheid. Twee universiteiten lichten toe dat momenteel wordt onderzocht welke elementen van kennisveiligheid terug kunnen komen in de bestaande trainingen en onboarding sessies. Ongeveer de helft van de universiteiten biedt nog geen (structurele) trainingen of wachten op de middelen die het landelijk Loket Kennisveiligheid/de Rijksoverheid aan het ontwikkelen is.

Het overgrote deel van de universiteiten biedt (nog) geen **opfrismodules** voor het zittende personeel. Zij geven aan dit nog niet te doen omdat ze pas net gestart zijn met de ontwikkeling van het kennisveiligheidsbeleid en/of nog in de implementatie van de bewustwordingsfase zitten en daarom nog niet aan een 'opfrismoment' toe zijn. Op twee universiteiten krijgen zittende medewerkers wel (herhaal)trainingen op diverse veiligheidsthema's. Deze trainingen zijn echter niet specifiek gericht op kennisveiligheid.

Geen van de universiteiten biedt speciale trainingsprogramma's gericht op academische kernwaarden voor **gastonderzoekers** of -studenten uit landen met een verhoogd risicoprofiel. Instellingen wijken op dit punt bewust af van de Leidraad, omdat ze het onwenselijk vinden om slechts een specifieke groep - op basis van nationaliteit - te trainen. Daarnaast zijn er geen gestandaardiseerde programma's voor gastonderzoekers. Bruikbaarder vindt men het uitgangspunt dat elke wetenschapper, ook buitenlandse (gast)onderzoekers, de Gedragscode Wetenschappelijke Integriteit onderschrijft en naleeft.

Naast het geven van trainingen en presentaties biedt een aantal universiteiten ook informatie over kennisveiligheid op een speciale website of middels thema-nieuwsbrieven. Instellingen gebruiken de websites voor het laagdrempelig toegankelijk maken van informatie over sanctielijsten, reisinformatie en/of andere informatie rondom kennisveiligheid. Op in ieder geval één instelling worden op de website ook voorbeelden van rode vlaggen gedeeld, zodat medewerkers een beeld krijgen in welke situaties aan de bel moet worden getrokken.

4.1.3 Dienstreizen naar het buitenland

Universiteiten zijn ook gevraagd naar hun beleid rondom dienstreizen naar landen met een verhoogd risicoprofiel. We zien dat veel universiteiten de reisadviezen vanuit het Ministerie van Buitenlandse Zaken volgen.[19] Een aantal universiteiten kiest ervoor om aanvullend op die reisadviezen handreikingen en/of procedures op te stellen. Denk hierbij aan het bieden van speciale reislaptops, expliciete toestemming van het College van Bestuur om te reizen naar landen met een oranje of rood reisadvies, een verplicht goedkeuringsproces of het aanbieden van pre-departure briefings. Bij een deel van de universiteiten (6 uit 14) is het beleid rondom dienstreizen nog in ontwikkeling of wordt het huidige beleid momenteel geëvalueerd.

19 Reisadviezen | Nederland Wereldwijd

4.2 Fysieke en digitale beschermingsmaatregelen

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

De meeste universiteiten (10 van de 14) hebben een **restrictief toegangsbeleid voor bepaalde ruimtes** (zoals afdelingen, gebouwen of labs). De andere vier universiteiten geven aan dat dit beleid in ontwikkeling is. Universiteiten zijn in beginsel openbare instellingen met vrije toegang voor personen, specifiek onderzoekers en studenten. Desalniettemin geldt voor met name labs met kostbare en/of kwetsbare apparatuur geregeld dat hiervoor restrictief toegangsbeleid is ontwikkeld. Dit toegangsbeleid is dan ook meestal niet ontwikkeld vanuit een kennisveiligheidsperspectief, maar dit wordt in toenemende mate meegewogen in het besluit voor restrictief toegangsbeleid voor bepaalde ruimten. In dit geval wort veelal een passcanner gebruikt, waardoor op individueel niveau kan worden bepaald tot welke ruimtes een medewerker toegang heeft. De afweging over het toegang verlenen aan een medewerker wordt bij een groot deel van de universiteiten op facultair niveau bepaald.

Meer dan de helft van de universiteiten geeft aan beleid te hebben voor de **toegang van buitenlandse reisdelegaties** tot afgesloten ruimtes. Een deel van de universiteiten geeft aan dat formeel beleid hiervoor nog in ontwikkeling is. Voor de meeste universiteiten geldt dat het beleid is dat buitenlandse reisdelegaties alleen toegang krijgen tot restrictieve ruimtes onder begeleiding van een medewerker met toegang tot die ruimte. Een aantal universiteiten geeft ook aan dat buitenlandse reisdelegaties helemaal geen toegang krijgen tot ruimtes met een restrictief toegangsbeleid.

4.2.2 Restrictief toegangsbeleid voor onderzoeksgegevens en documenten

Het merendeel van de universiteiten (10 van de 14) geeft aan dat ze beleid hebben omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten. Bij veruit de meeste universiteiten is er centraal beleid maar is de data eigenaar / onderzoeker verantwoordelijk voor het juist oormerken en omgaan met de data. Negen universiteiten geven aan beleid te hebben voor het rubriceren van documenten, denk aan labels als ‘vertrouwelijk’ of ‘geheim’. Andere universiteiten geven aan dat rubricering van documenten case-by-case wordt toegepast, of dat dit niet van toepassing is binnen de eigen instelling, waardoor er geen behoefte bestaat aan beleid hierop.

De relevantie van toegang tot digitale omgevingen en data voor kennisveiligheidsbeleid betekent dat er nauwe samenhang is met het **cyberveiligheidsbeleid** van universiteiten. Geregeld zijn medewerkers van cyberveiligheid dan ook betrokken bij kennisveiligheidsbeleid en is de CISO (Chief Information Security Officer) betrokken bij het adviesteam (zie hierboven). Beide thema’s worden gezien als onderdeel van een integrale aanpak binnen de instelling. 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

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

hoger onderwijs 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

We observeren in dit onderzoek geen dilemma's op het vlak van risicomanagement. Wel worden twee aandachtspunten genoemd: (1) het belang van bewustzijn op alle lagen van de organisatie en (2) het voorkomen van onnodige bureaucratie.

Universiteiten zijn decentraal opgezet met veel autonomie op het niveau van faculteiten en onderzoekers. Het is dus niet goed mogelijk om eenduidig top-down kennisveiligheidsbeleid te implementeren. Universiteiten geven dan ook aan dat het van belang is om **kennisveiligheidsbewustzijn** te creëren op alle lagen binnen de organisatie.

Kennisveiligheidsbeleid, vastgelegde processen en protocollen kunnen helderheid scheppen voor het signaleren en mitigeren van kennisveiligheidsrisico's. Universiteiten 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 is daarom punt van discussie voor met name de brede universiteiten. Zij ervaren hierop weinig richting en handvatten vanuit de overheid hoe onderzoek in de alfa- en gammawetenschappen zich dient te verhouden tot kennisveiligheid. In de verdiepende casestudy bij één brede universiteit wordt dan ook aangegeven dat zij voornamelijk inzetten op informeel beleid met een sterke nadruk op het creëren van voldoende kennisveiligheidsbewustzijn, in plaats van afhankelijkheid van formele processen en protocollen.

4.4 Lessons learned

4.4.1 Centraal adviesteam

Meerdere universiteiten 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, stellen checklists op waar naar te kijken bij het controleren van een cv, maken risico-inschattingen, vergroten draagvlak binnen de organisatie om met kennisveiligheid aan de slag te gaan en adviseren bij twijfelgevallen. Universiteiten geven terug dat het prettig is om de kennis en kunde rondom kennisveiligheid binnen een adviesteam te beleggen en dat de korte lijnen tussen HR en het adviesteam de werkprocedures en het maken van keuzes in het geval van twijfel over een casus versnelt.

Het draagvlak van kennisveiligheidsbeleid neemt ook toe als beleid binnen de logica van huidige processen op de werkvloer komt te liggen. Verschillende universiteiten combineren kennisveiligheid

---

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.

binnen overkoepelend beleid op integrale veiligheid, bijv. in combinatie met ethische toetsing en cyberveiligheid.

4.4.2 Bewustzijn

Ook rondom het bevorderen van bewustzijn delen universiteiten geleerde lessen.
Eén van de universiteiten geeft aan een goede balans te bieden tussen bewustwordingscampagnes op aanvraag (bijvoorbeeld wanneer een casus speelt, of wanneer een spreker vanuit het adviesteam wordt gevraagd bij een themaoverleg), maar daarnaast als centraal adviesteam ook zelf initiatief te nemen voor het organiseren van kennissessies rondom kennisveiligheid. Op die manier blijft het thema geborgd binnen de organisatie.

Meerdere universiteiten geven aan dat het belangrijk is om meerdere lagen binnen de universiteit op de hoogte te houden van het thema kennisveiligheid, zodat de verantwoordelijkheid en kennisopbouw rond het thema niet bij één afdeling of één groep werknemers ligt. In ieder geval één universiteit geeft aan de presentaties rondom kennisveiligheid in verschillende gremia met regelmaat te herhalen, met als doel de kennisopbouw rondom het thema zo goed mogelijk te borgen. Universiteiten vinden het nuttig om in hun presentaties ook concrete handvatten te bieden waarmee vraagstukken kunnen worden opgepakt. Wel geven universiteiten aan dat het belangrijk is om te investeren in een cultuur van bewustzijn zonder daarbij onnodig onrust te creëren. Het zoeken naar een goede balans daartussen is een uitdaging.

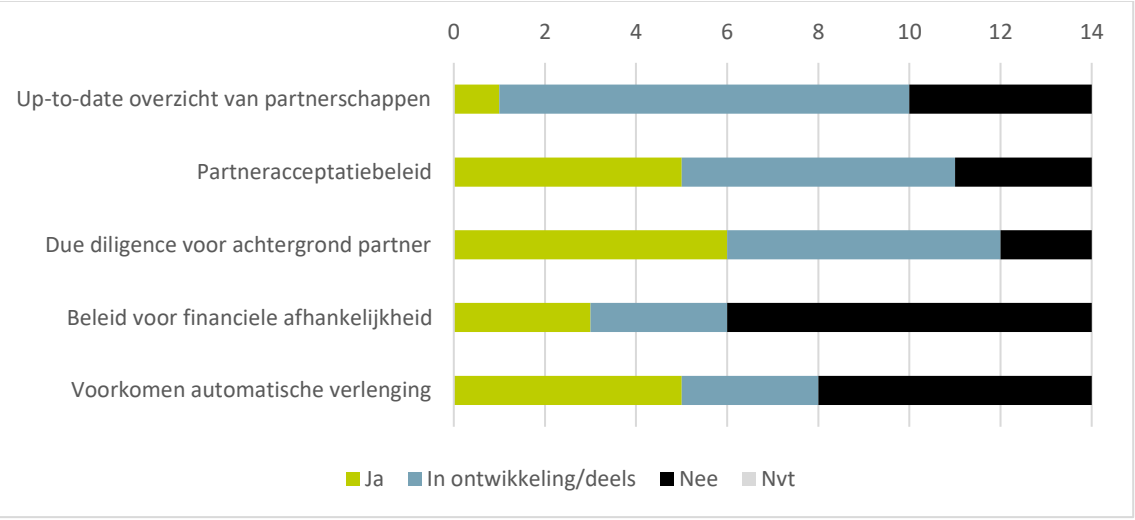
5 Internationale partnerschappen en juridische kaders

In dit hoofdstuk analyseren we het kennisveiligheidsbeleid omtrent internationale samenwerking. In paragraaf 5.1 behandelen we concrete partnerschappen en samenwerkingsverbanden die Nederlandse universiteiten aangaan met internationale organisaties en individuen. Daarna bespreken we in paragraaf 5.2 de omgang met juridische kaders en gedragscodes voor internationale partnerschappen, zoals exportregels en sanctieregimes. In paragraaf 5.3 bespreken we de dilemma's en uitdagingen specifiek op dit onderdeel van het kennisveiligheidsbeleid, gevolgd door best practices en geleerde lessen in paragraaf 5.4.

5.1 Internationale partnerschappen

De meeste universiteiten (9 van de 14) geven aan dat het beleid rondom internationale partnerschappen nog in ontwikkeling is. In de volgende paragrafen gaan we in op de verschillende onderdelen van het beleid. Figuur 5.1 geeft een overzicht van de activiteiten van universiteiten ten aanzien van internationale partnerschappen en samenwerkingsverbanden die zij aangaan met organisaties en individuen, waarbij inhoudelijke of financiële toezeggingen worden gedaan en overeenkomsten worden afgesloten.

Figuur 5.1 Overzicht activiteiten internationale partnerschappen



5.1.1 Overzicht partnerschappen en financiering

Om (instellingsbreed) kennisveiligheidsbeleid te maken op internationale partnerschappen, is het van belang dat er zicht is op de internationale partnerschappen. Bij verreweg de meeste universiteiten (9 van de 14) is een centraal overzicht van veiligheidsgevoelige partnerschappen nog in ontwikkeling. Instellingen noemen een aantal redenen waarom dergelijke overzichten nog niet bestaan.

De informatie is vaak **gefragmenteerd** aanwezig in de organisatie. Universiteiten zijn grotendeels decentraal opgezet, met veel autonomie op het niveau van faculteiten. Dit houdt in dat er geen gestandaardiseerde registratie van samenwerkingen in een centraal doorzoekbaar systeem is. Verschillende universiteiten stellen dat College van Besturen niet noodzakelijk op de hoogte hoeven te

zijn van alle samenwerkingen, maar dat het wenselijk is als actuele overzichten gemaakt kunnen worden. Hierbij wordt door een enkele universiteit aangegeven dat dergelijke overzichten dan beperkt kunnen zijn tot de samenwerkingspartners van buiten de EU, of alleen voor samenwerkingspartners uit landen met een hoog risicoprofiel.

Dit leidt tot een tweede aandachtspunt, namelijk hoe te bepalen wanneer sprake is van een buitenlandse samenwerkingspartner, vooral in het geval van bedrijven. Internationale bedrijven hebben veelal ook een **Europese (of zelfs Nederlandse) vestiging**. In dat geval moet eveneens in beeld worden gebracht waar het moederbedrijf van een samenwerkingspartner is gevestigd. Een andere uitdaging zit in de deelname aan internationale consortia. Dergelijke consortia kunnen bestaan uit tientallen partijen, waardoor het lastig is om overzicht te houden met wie de universiteit precies samenwerkt.

Ten derde houden sommige universiteiten weliswaar een centraal up-to-date overzicht van partnerschappen bij, maar worden daarin **kennisveiligheidsrisico's** niet meegenomen en geregistreerd. Een dergelijk overzicht wordt door een enkele universiteit wel handmatig gecheckt op mogelijke kennisveiligheidsrisico's. Deze universiteiten streven er naar om ook hiervoor registratie aan te brengen.

Enkele universiteiten geven aan dat zij geen centraal overzicht van internationale partnerschappen ontwikkelen. Deze universiteiten hebben ervoor gekozen om de verantwoordelijkheid hiervoor exclusief decentraal te beleggen. Het is aan de faculteiten om partnerschappen te registreren, en om te bepalen op welk detailniveau dit gedaan wordt. Decentrale registraties kunnen voor het CvB inzichtelijk worden gemaakt, maar deze overzichten zijn moeilijk onderling vergelijkbaar, en bevatten ook (nog) geen kennisveiligheidsinformatie, maar enkel informatie over financieringsbronnen.

Meerdere universiteiten benoemen dat het overzicht dat er is (al dan niet volledig of (de)centraal) actueel wordt gehouden door periodieke controles van het overzicht. Deze universiteiten streven naar een routine waarbij elk partnerschap, inclusief financiering en mogelijke kennisveiligheidsinformatie standaard geregistreerd wordt, waardoor een continu up-to-date overzicht ontstaat. Enkele universiteiten zijn ook voornemens om in deze routine informatie over buitenlandse promovendi en gastwerknemers op te nemen (hierover meer in hoofdstuk 6).

We zien geen eenduidig beeld van beleid op individuele samenwerkingen. Een wetenschapper kan besluiten om een analyse uit te voeren of artikel te publiceren met een wetenschapper in het buitenland, zonder dat hiervoor op institutioneel niveau een samenwerking wordt aangegaan. In dit geval heeft de instelling geen zicht op de samenwerking. Het is dan van belang dat wetenschappers zelf voldoende kennisveiligheidsbewust zijn (zie paragraaf 4.1.2).

5.1.2 Partneracceptatiebeleid (due diligence)

In deze paragraaf bespreken we hoe het partneracceptatiebeleid van universiteiten er uit ziet, hoe dit proces wordt uitgevoerd en welke *tools* universiteiten hiervoor gebruiken. Vijf universiteiten geven aan een partneracceptatiebeleid te hebben. Bij zes universiteiten is dit nog in ontwikkeling; drie universiteiten geven aan hier momenteel niet mee bezig te zijn. Daarnaast geven zes universiteiten aan dat zij voor mogelijke partners *due diligence* verrichten; 6 universiteiten geven aan dit beleid te ontwikkelen, en 2 universiteiten geven aan dit niet te doen.

Als due diligence op kennisveiligheidsgebied nodig is, moet eerst een (potentieel) kennisveiligheidsrisico gesignaleerd worden. Universiteiten geven aan dat idealiter de wetenschapper of groep die de

samenwerking aan wil gaan hierin een signalerende functie heeft aan het begin van het proces. In dat geval worden mogelijke risico's namelijk zo vroeg mogelijk gesignaleerd. Als een wetenschapper of onderzoeksgroep signaleert dat een samenwerking mogelijk kennisveiligheidsgevoelig is, kan deze de juiste kanalen (zoals het adviesteam) inschakelen. Als dit niet gebeurt, zijn er nog andere manieren waarop kennisveiligheidsrisico's in een samenwerking gesignaleerd kunnen worden. Dit kunnen bijvoorbeeld beleidsmedewerkers internationalisering van de faculteit, graduate school of centrale organisatie doen. Bij uiteindelijke ondertekening van het contract heeft de desbetreffende juridische afdeling (facultair of centraal) ook nog een signalerende functie.

Due diligence van mogelijke samenwerkingen wordt door universiteiten in de regel case-by-case uitgevoerd, waarbij verschillende universiteiten kaders en richtlijnen hanteren om te bepalen hoe de beoordeling procesmatig verloopt. Bij de meeste universiteiten wordt het adviesteam betrokken bij de beoordeling. Eén universiteit geeft aan dat de initiator van de samenwerking wordt gevraagd om een vragenlijst in te vullen, waaruit moeten blijken of een verdere risicoanalyse nodig is. Het verschilt tussen universiteiten of de eindverantwoordelijkheid en beslissingsbevoegdheid voor het aangaan van samenwerkingsverbanden ligt bij het College van Bestuur, faculteitsbestuur, dienstdirecteur of afdelingshoofd.

De overwegingen die gemaakt worden in het kader van due diligence zijn over het algemeen dezelfde tussen de universiteiten. Universiteiten 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:
  - Het doel van de samenwerking, hoe realistisch deze doelen zijn, de vorm van de samenwerking en de motivatie achter de samenwerking.
  - De sensitiviteit van het kennisgebied en onderzoeksonderwerp waarop de samenwerking plaatsvindt.
  - Het Technology Readiness Level (TRL) van het onderzoek.
  - Juridische bepalingen (zie paragraaf 5.2).
- Financiën. Hoe meer geld er met een samenwerking gemoeid is, hoe centraler en hoger de verantwoordelijkheid en beslissingsbevoegdheid ligt. Kleinere samenwerkingsverbanden worden vooral op decentraal niveau beoordeeld en ondertekend.
- De samenwerkingspartner. Universiteiten letten hier op de academische status en de achtergrond van de samenwerkingspartner. Waar mogelijk wegen universiteiten resultaten van reeds bestaande samenwerking met deze partner. Ook het kennisveiligheidsrisicoprofiel van de beoogde samenwerkingspartner wordt hier meegenomen, bijv. op basis van de ASPI-lijst.

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

- Het Kader Kennisveiligheid van UNL.
- Het toetsingskader internationale samenwerking en veiligheid.
- De Veiligheidstoets Investeringen Fusies en Overnames (VIFO).
- Sanctiewetgeving EU en de OFAC.
- Informatie over compliance regels van de Nederlandse banken ten aanzien van betalingsverkeer.
- De Nederlandse gedragscode wetenschappelijke integriteit[23].

[23] KNAW, NFU, NWO, TO2, VH, UNL (2018) Nederlandse gedragscode wetenschappelijke integriteit

- Compliance en due diligence data van Altares, Dun & Bradstreet.
- De ASPI-lijst (specifiek voor samenwerkingsverbanden met Chinese instellingen)[24].
- De vastgestelde lijst met Key Enabling Technologies als referentielijst voor sensitieve technologieën.

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. Drie universiteiten hebben beleid rondom dit thema, en drie zijn dit aan het ontwikkelen. Ruim de helft van de universiteiten (8 van de 14) geeft aan geen beleid te hebben om te voorkomen dat ze in een staat van financiële afhankelijkheid worden gebracht.

Een expliciete reden die universiteiten hiervoor geven is dat externe financiering een beperkt deel uitmaakt van de totale financiering van universiteiten, faculteiten en instituten. In 2021 was gemiddeld ongeveer 15% van de inkomsten van universiteiten afkomstig uit externe financiering, van zowel internationale organisaties, nationale overheden, overige non-profitorganisaties en bedrijven.[25] Omdat het leeuwendeel van de financiële middelen van universiteiten dus van de Nederlandse rijksoverheid – NWO inbegrepen – komt, is op institutioneel niveau geen sprake van financiële afhankelijkheid. Een enkele universiteit geeft aan dat financiële afhankelijkheid per definitie ontstaat wanneer een project gefinancierd wordt vanuit externe middelen; dit project had anders immers geen doorgang kunnen vinden. Dergelijke zorgen over (mogelijke) afhankelijkheid van onderzoekers en onderzoeksgroepen van externe financiering spelen in bredere zin en zijn niet beperkt tot kennisveiligheid.[26]

Meerdere universiteiten geven aan expliciet aandacht te hebben voor extern gefinancierde studenten en promovendi. Zo wordt beleid ontwikkeld om te diversifiëren hoe promovendi worden gefinancierd en kennen sommige instellingen een maximum aan extern gefinancierde studenten en promovendi. Dit aantal is bij verschillende universiteiten dan ook aan het afnemen. Dit aspect bespreken we verder in hoofdstuk 6.

5.1.4 Voorkomen automatische verlenging

Als samenwerkingsverbanden reeds bestaan, is het niet wenselijk dat deze automatisch verlengd worden 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.
Vijf universiteiten geven aan dat ze beleid hebben om automatische verlengingen van internationale partnerschappen te voorkomen, drie universiteiten zijn dit aan het ontwikkelen en zes universiteiten geven aan zulk beleid niet te hebben en ook niet te gaan ontwikkelen.

De meeste samenwerkingsverbanden vinden plaats in een onderzoekscontext. Onderzoeksprojecten hebben daarbij een natuurlijk einde bij afronding van het project. Bij tijdelijke contracten waarvan verlenging wel logisch is moet dit wel expliciet worden overeengekomen, wat niet automatisch gebeurt.

---

[24] Home – Chinese Defence Universities Tracker — ASPI

[25] Baten Nederlandse universiteiten, werk voor derden | Rathenau Instituut

[26] Zie bijvoorbeeld De Jonge Akademie (2023). Denkruimte. Een analyse van structurele bedreigingen voor academische vrijheid en integriteit.

Bij institutioneel partnerschap (veelal een Memorandum of Understanding) uiten instellingen de ambitie om meer samen te werken in onderwijs en onderzoeksprojecten. Om in deze gevallen automatische verlenging te voorkomen zijn meerdere universiteiten bezig met het vormgeven van contractbeheer waarin betrokkenen automatisch gealerteerd worden ruim voor het verlengmoment. Dit hangt samen met de mate waarin overzichten van internationale samenwerkingen kunnen worden gecreëerd (zie hierboven). Enkele universiteiten voeren reeds beleid om in een Memorandum of Understanding expliciet aan te geven op welke kennisgebieden kan worden samengewerkt in onderwijs en onderzoek.

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. Om compliant te zijn met exportcontroles en regels is het allereerst nodig dat bepaald wordt wanneer een technologie dual-use is. De exportregels voor dual-use technologieën zijn echter ingewikkeld en vragen om interpretatie. Het bepalen van mogelijke dual-use toepassingen is in grote mate afhankelijk van de kennis van de individuele onderzoeker. Deze heeft de expertise van het onderzoeksonderwerp en de mogelijke impact ervan. De individuele onderzoeker moet hierbij echter samenwerken met de (juridische) afdelingen of medewerker(s) met kennis van de exportregels. Deze samenwerking is nog niet een natuurlijk gegeven. De institutionele afhankelijkheid van de individuele onderzoeker is kwetsbaar, omdat het niet in het belang van de onderzoeker is om onderzoek als dual-use aan te merken. Dit benadrukt het belang van kennisveiligheidsbewustzijn onder onderzoekers (zie paragraaf 4.1.2). Verschillende universiteiten ontwikkelen ondersteunende functies die waar nodig de afweging kunnen (helpen) maken en adviesvragen inwinnen bij het loket Kennisveiligheid, de KvK en de Centrale Dienst voor In-en Uitvoer (CDIU) van de Douane. Voor dual-use-goederen in de categorie van Biologische Agentia hanteren universiteiten al de Richtlijn Veilig Werken met Biologische Agentia. Dit gaat nog op case-by-case basis.

Meerdere universiteiten geven aan dat compliance met exportregels niet geborgd is, en daar ook geen beleid voor in ontwikkeling te hebben. Dit zijn voornamelijk brede universiteiten die, in tegenstelling tot technische universiteiten, aangeven weinig tot geen dual-use technologieën te onderzoeken. Universiteiten die wel mogelijk dual-use onderzoek verrichten geven aan dat dit alsnog niet (altijd) onder exportregels valt, omdat fundamenteel onderzoek met een TRL van 1 of 2 vrijgesteld is van exportregels.[27] Uitzondering hierop is onderzoek dat wordt gefinancierd door of voor militair eindgebruik.

[27] Zie Aanbeveling (EU) 2021/1700 van de commissie van 15 september 2021 inzake interne nalevingsprogramma's voor controles op onderzoek met betrekking tot producten voor tweeërlei gebruik uit hoofde van Verordening (EU) 2021/821 van het Europees Parlement en de Raad 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik. EUR-Lex - 32021H1700 - EN - EUR-Lex (europa.eu)

5.2.2 Compliance met niet-EU import- en exportregels

Ook landen buiten de EU hebben import- en exportregels die voor Nederlandse universiteiten relevant kunnen zijn. Het meest genoemde voorbeeld op dit gebied is de extraterritoriale werking van Amerikaanse sancties en regelgeving. Dit geldt vooral voor 're-export' van (componenten of software van) apparatuur van Amerikaanse origine. Ook op het gebied van deze exportregels is bij veel universiteiten nog geen institutionele borging in beleid, voornamelijk omdat hier niet structureel sprake van is en dit dus op case-by-case basis kan worden afgehandeld.

5.2.3 Compliance met internationale en EU-sanctieregimes

Compliance met sanctieregimes is bij universiteiten nog weinig institutioneel geborgd in beleid. Sommige universiteiten geven aan ook hier case-by-case mee om te gaan, of dat de verantwoordelijkheid vooral op decentraal niveau ligt. Faculteiten gebruiken hiervoor de expertise van HR, de International Office, Juridische zaken, het adviesteam kennisveiligheid en Student Affairs in het geval van studenten die komen uit landen waarvoor sancties gelden. Een enkele universiteit geeft aan dat voor onderzoek dat valt onder het Missile Technology Control Regime (MTCR) een aanvraag moet worden gedaan bij de Rijksoverheid. Daarnaast geven universiteiten aan in de toekomst vaker RVO te willen inschakelen om gebruik te maken van informatie over sancties. Ook hier wordt kennisveiligheidsbewustzijn onder onderzoekers genoemd als belangrijk instrument voor compliance.

5.2.4 Gedragscodes

Gedragscodes zijn niet-bindende richtinggevende richtlijnen die universiteiten kunnen helpen bij het maken van afwegingen. Voorbeelden hiervan zijn de Leidraad, het Kader Kennisveiligheid Universiteiten[28] en de EU guidelines on Tackling R&I foreign interference[29]. Daar voegen sommige universiteiten hun eigen interne gedragscodes aan toe, bijvoorbeeld integriteits- of anti-corruptiecodes om gedragscodes herkenbaarder te maken voor werknemers. Dit leidt volgens universiteiten tot beter gebruik van de gedragscode. Sommige van deze interne gedragscodes zijn nu specifiek gericht op een land (China), maar worden landenneutraal gemaakt.

Vrijwel alle universiteiten verwerken deze codes in een eigen kader of richtlijn, of vertalen het in hun kennisveiligheidsbeleid. Een eigen kader heeft volgens verschillende universiteiten de voorkeur, omdat dit qua stijl herkenbaarder is voor werknemers, en daardoor sneller gebruikt zal worden. Deze gedragscodes worden gebruikt om bewustzijn te vergroten binnen de organisatie.

5.3 Dilemma's en aandachtspunten

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

Het is voor universiteiten **niet altijd mogelijk om het risicoprofiel te bepalen** van samenwerkingspartners. Door sommige samenwerkingspartners wordt gewerkt met parapluconstructies waardoor de samenwerkingspartner op papier een andere organisatie is dan de samenwerkingspartner in de praktijk. Daarnaast is het niet duidelijk hoe om te gaan met dochterbedrijven van grote internationale bedrijven. Een voorbeeld wat genoemd wordt is bijvoorbeeld

---

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

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

Huawei Zweden wat weliswaar gevestigd is in Zweden (en daarmee een Europees bedrijf is), maar waarvan het moederbedrijf in China is gevestigd.

Daarbij zien universiteiten nog geregeld **tegenstrijdige adviezen**, waar een samenwerking met een buitenlandse universiteit of bedrijf door het ene overheidsinstituut wordt afgeraden, terwijl deze wordt gestimuleerd door een ander overheidsinstituut. Zeker waar onderzoek vaak in consortia wordt uitgevoerd en op basis van Europese financiering, zien onderzoekers verschillen in de richtlijnen die landen meegeven. Verschillende universiteiten vrezen een (inter)nationaal waterbedeffect, waarbij strenge richtlijnen op kennisveiligheid binnen de eigen instelling of het eigen land simpelweg ertoe leiden dat risicovolle samenwerkingen worden aangegaan door andere instellingen in Nederland of Europa.

Het is voor universiteiten daarnaast ingewikkeld om beleid te ontwikkelen op **individuele samenwerking**. Wetenschappers werken autonoom en kunnen zelfstandig een persoonlijke samenwerking aangaan. De nadruk in het kennisveiligheidsbeleid ligt voor universiteiten daarom op (het screenen van) institutionele samenwerkingen. De Leidraad maakt dit onderscheid niet en gaat uit van kennisveiligheidsbeleid op alle samenwerking, maar geeft geen handvatten voor beleid op individuele samenwerking.

Ook voor compliance met **juridische kaders** geldt dat dit afhankelijk is van individuele onderzoekers voor het signaleren van onder meer 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

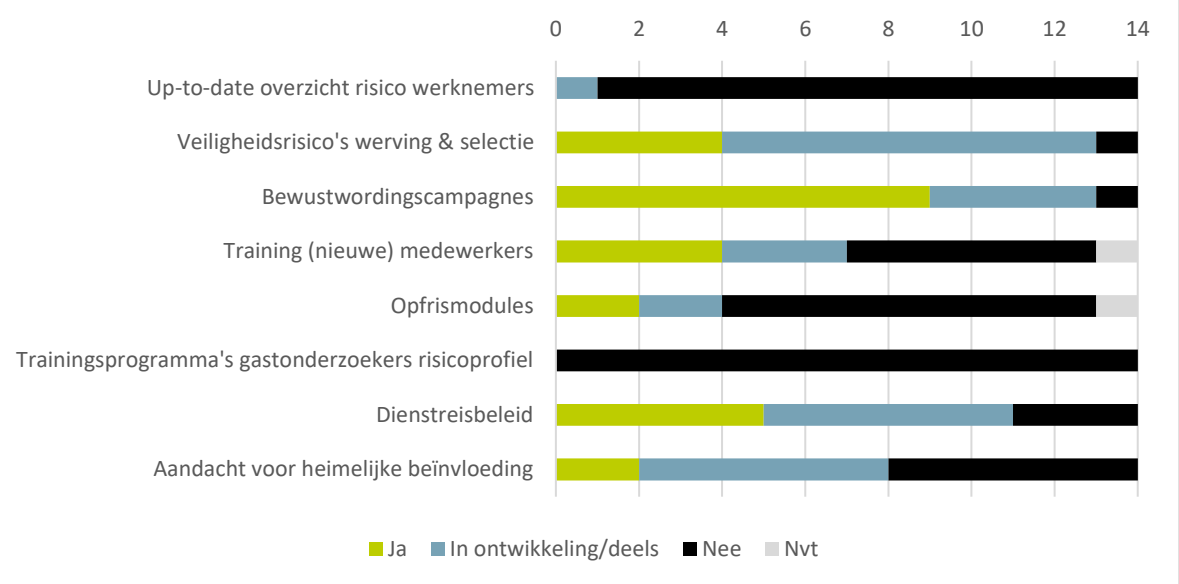
Kennisveiligheid in internationale samenwerking en compliance met juridische kaders laat zich niet goed vatten in afvinklijstjes. Dit wordt al genoemd in het AWTI-rapport en wordt hier door universiteiten beaamd. Dit komt doordat vakgebieden, instellingen en partnerschappen dusdanig verschillen dat generiek beleid lastig vorm te geven is. Veel kennisveiligheidscasuïstiek is volgens universiteiten dusdanig specifiek dat dit niet goed te vatten is in generiek beleid, daarom wordt gekozen voor case-by-case behandeling. Essentieel hiervoor is dat kennisveiligheidsbewustzijn in de gehele organisatie aanwezig is, omdat anders risico's ten aanzien van onderzoek en samenwerkingspartners niet goed kunnen worden gesignaleerd en adequaat beoordeeld.

6 Personeelsbeleid

De Leidraad stelt dat het wenselijk is dat kennisveiligheid onderdeel wordt van het personeelsbeleid. In paragraaf 6.1 beschrijven we op welke manier kennisveiligheid is geïmplementeerd in verschillende onderdelen van het personeelsbeleid van de universiteiten. 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 in paragraaf 6.2 en 6.3 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

Het overgrote deel van de universiteiten (12 van de 14) geeft aan dat het kennisveiligheidsbeleid van hun instelling met betrekking tot personeelsbeleid en gedragscodes nog in ontwikkeling is. Eén universiteit geeft aan (nog) helemaal geen kennisveiligheidsbeleid met betrekking tot personeelsbeleid te hebben, een andere geeft aan dat het personeelsbeleid is vastgesteld en dat de uitvoering ervan aantoonbaar is. Zie Figuur 6.1 voor een overzicht van kennisveiligheidsactiviteiten rondom personeelsbeleid van universiteiten.



Figuur 6.1 Overzicht activiteiten personeelsbeleid

6.1.1 Overzicht (gast)werknemers

We vroegen universiteiten 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*. Dertien van de veertien deelnemende universiteiten gaven nadrukkelijk aan dit niet te doen. Zij geven aan dat er geen juridische basis is voor een dergelijke lijst. Ook behoort het opsporen of identificeren van werknemers, gasten en gastwerknemers die een mogelijk risico voor de (kennis)veiligheid vormen, niet tot de opdracht van een universiteit .

Eén universiteit geeft aan op centraal niveau wel een overzicht bij te houden van alle (gast)werknemers, maar daarbij niet bij te houden wie van hen een risico vormt voor kennisveiligheid. Dit up-to-date overzicht van (gast)werknemers wordt op deze universiteit alleen bijgehouden binnen faculteiten waar onderzoek wordt gedaan op sensitieve kennisgebieden.

De Leidraad geeft als advies “een dashboard [op bestuursniveau], een centraal overzicht van veiligheidsgevoelige partnerschappen, financiering en buitenlandse promovendi en gastonderzoekers” (p. 36). In dit onderzoek is dit advies vertaald naar de vraag naar een overzicht van werknemers, gasten en gastwerknemers die een risico vormen op het gebied van kennisveiligheid. In de toelichting op de beantwoording dat dergelijke overzichten door bijna geen universiteit worden gemaakt wordt aangegeven dat dit advies betrekking heeft op kwantitatieve inzichten van studentmobiliteit, internationale promovendi en gastonderzoekers (d.w.z. aantallen studenten, promovendi en gastonderzoekers uit diverse landen). Het advies zou geen betrekking hebben op overzichten op persoonsniveau. Het verhelderen van dit onderscheid is een verbeterpunt voor eventuele vervolgmetingen.

Werving en selectieprocedure

13 van de 14 universiteiten 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. Negen universiteiten zijn nog bezig met de ontwikkeling van richtlijnen rondom kennisveiligheid voor de werving en selectiefase.

Universiteiten zoeken in deze ontwikkelfase naar verschillende manieren om kennisveiligheid mee te nemen in de werving en selectieprocedure. Twee universiteiten toetsen bijvoorbeeld alleen de achtergrond van een deel van het nieuwe personeel, bijvoorbeeld alleen personeel met een beurs uit het buitenland, of alleen kandidaten die solliciteren op functies binnen faculteiten of groepen waar kennisveiligheidsrisco’s spelen. Tenminste één universiteit kondigt in vacatures aan dat een kennisveiligheidscheck onderdeel kan uitmaken van de selectieprocedure.

Een aantal universiteiten is bezig met een pilot rondom achtergrondtoetsing of verkent momenteel of en hoe achtergrondtoetsing in de wervingsfase een haalbare optie is. Twee universiteiten laten de inschatting of de kandidaat een mogelijk risico vormt voor de kennisveiligheid bij het wervende personeel/onderzoekers zelf en geeft het personeel daarbij de mogelijkheid om (ad hoc) advies in te winnen bij het adviesteam kennisveiligheid. Andere universiteiten kiezen ervoor om geen nieuwe medewerkers aan te nemen die van een hoog-risico universiteit afkomstig zijn, of vragen Nederlandse sollicitanten voor ondersteunende functies om een Verklaring Omtrent het Gedrag (VOG).

6.1.2 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. Universiteiten zijn zich bewust van de risico’s op heimelijke beïnvloeding. Twee universiteiten geven aan eerder al signalen te hebben opgevangen vanuit promovendi. Deze signalen vormden voor hen aanleiding om beleid op te stellen rondom dit thema.

De manier waarop universiteiten omgaan met dit thema verschilt sterk. In ieder geval twee universiteiten benoemen expliciet dat er meldpunten en aanspreekpunten beschikbaar zijn waarbij

(internationale) medewerkers die zich niet veilig voelen terecht kunnen. Denk hierbij aan vertrouwenspersonen, integriteitscoördinatoren en *international offices*. Eén universiteit heeft de begeleiding verstevigd voor onderzoekers die zich in een mogelijk kwetsbare positie bevinden en wijst nieuwe onderzoekers al in de selectieprocedure op de risico's voor familie in het thuisland. Eén universiteit geeft aan bewustwordingscampagnes te gaan voeren rondom heimelijke beïnvloeding in de verwachting dat supervisors daarmee alerter worden op de manier waarop medewerkers door statelijke actoren kunnen worden beïnvloed. Uit de verdiepende gesprekken maken we op dat universiteiten zich bewust zijn van de kwetsbare positie waarin personeel zich geplaatst kan zien en dat onderzoekers die onderzoek doen naar een gevoelig onderwerp, potentieel onder druk kunnen worden gezet worden door statelijke actoren.

Zes universiteiten hebben op dit moment geen specifiek beleid ontwikkeld rondom heimelijke beïnvloeding. Twee universiteiten geven aan het stigmatiserend, veroordelend en/of discriminerend te vinden om beleid op te stellen voor een specifieke groep medewerkers. Drie universiteiten geven een andere reden. Eén van deze drie universiteiten geeft aan dat het niet bij hun maatschappelijke opdracht hoort om hier beleid voor op te stellen en vertrouwt in dit kader op de kennis en kunde van de veiligheidsdiensten. Een andere universiteit weet (nog) niet goed hoe beleid op te stellen rondom dit thema en de derde universiteit wil in overleg met andere Nederlandse universiteiten bezien hoe en onder welke voorwaarden ze met beurspromovendi willen doorgaan.

6.2 Dilemma's en aandachtspunten

Op veel universiteiten spelen dilemma's rondom personeelsbeleid. 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

Universiteiten 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. Meerdere universiteiten geven in dat kader aan dat het generiek weren van mensen met een specifieke nationaliteit wettelijk niet toegestaan is (discriminatieverbod).[30] Bovendien vinden ze het onwenselijk, omdat het leidt tot een cultuur van uitsluiting. Als het gaat over samenwerkingen met instellingen of onderzoekers uit specifieke landen ligt stigmatisering snel op de loer. Medewerkers in de kennisveiligheidsketen nemen soms snel het zekere voor het onzekere ("dan nemen we maar helemaal geen Russen of Iraniërs meer aan"), terwijl men het ook erover eens dat dit onwenselijk is.

Universiteiten laten weten dat ze de nationaliteit van sollicitanten niet mee willen en mogen wegen in selectieprocedures. In meerdere gesprekken komt dan ook naar voren dat universiteiten geen vacatureteksten opstellen waarin afkomstcriteria zijn opgenomen. Meerdere universiteiten geven daarnaast aan behoefte te hebben aan een landelijk kader waarin relevante en juridisch houdbare risicofactoren zijn opgenomen die kunnen worden meegewogen bij een selectie van personeel. Eén universiteit noemt daarbij dat het nemen van beslissingen op basis van onderbuikgevoelens gevaarlijk is,

30 Hierbij wordt regelmatig 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))

ook omdat ze daarmee als instelling het risico te lopen te discrimineren op basis van nationaliteit of etniciteit.
Ook het benoemen van risicolanden tijdens bewustwordingspresentaties kan stigmatiserend zijn en tot onveiligheid leiden. Volgens een betrokkene worden in presentaties regelmatig risicolanden genoemd van waaruit een deel van het aanwezige publiek afkomstig is. Dat is voor zowel de universiteit als de werknemers ongemakkelijk. Een andere betrokkene geeft aan dat onderzoekers uit risicolanden zelf al aangeven het inmiddels gewend te zijn om eruit te worden gepikt.

Gevoelens van discriminatie en uitsluiting komen tot slot ook naar voren wanneer beleidsmaatregelen en sancties richting bepaalde landen worden aangescherpt. Wat eerder wel mogelijk was, kan onder aangescherpte maatregelen soms ineens niet meer. Universiteiten geven aan dat deze aangepaste overwegingen lastig uit te leggen zijn aan nieuwe kandidaten, zeker wanneer een universiteit eerder wel mensen uit een bepaald land in dienst heeft genomen - mogelijk zelfs personeel dat onder de huidige sancties niet door screening- of toetsingsprocedures zou komen. Aangepast beleid wringt bijvoorbeeld sterk in het geval een wetenschapper één of meerdere sollicitanten uit het persoonlijke netwerk aandraagt en deze als gevolg van aangepaste sancties niet door de toetsingsprocedure komt of komen.

6.2.2 Achtergrondtoetsing[31]

Het toetsen van de achtergrond van nieuw personeel is een onderwerp dat zowel in de beantwoording van de vragenlijsten als in de verdiepende gesprekken tot discussie leidt. Over het algemeen zijn universiteiten zich bewust van de kennisveiligheidsrisico's, maar worstelen ze met de manier waarop ze hiermee om moeten en kunnen gaan. Abstract nationaal beleid vertaalt zich binnen de instellingen tot impact op het individuele niveau van veelbelovende sollicitanten en gewaardeerde collega's, wat betrokkenen binnen instellingen (onderzoekers, bestuurders en HR) in een lastige positie plaatst.

Universiteiten geven aan momenteel onvoldoende (personele) capaciteit en middelen in handen te hebben voor een adequate risico-inschatting van samenwerkingen of personen. Universiteiten wegen nu in veel gevallen kennisveiligheidsrisico's af op basis van spaarzaam beschikbare informatie. Er is bijvoorbeeld geen informatie beschikbaar over het persoonlijke netwerk van een kandidaat, waardoor de risicoschatting alleen globaal uitgevoerd kan worden op affiliatie-risico. Ook geven universiteiten aan dat onduidelijk is hoe ver hun verantwoordelijkheden en mogelijkheden strekken. Universiteiten vragen zich bijvoorbeeld af wat je AVG-technisch mag opvragen, hoe ver je moreel gezien terug mag graven in het werkverleden van een onderzoeker en vinden het lastig te bepalen wie je wel en niet moet toetsen zonder heel duidelijke wettelijke kaders. Een aantal universiteiten wijst in deze context op de maatschappelijke opdracht van de veiligheidsdiensten en zien liever dat deze diensten kandidaten screenen voor posities waar kennisveiligheidsrisico's aan zijn verbonden. Wel geeft in ieder geval één universiteit aan duidelijkheid te willen hebben op welke overwegingen een veiligheidsdienst hun adviezen of beslissingen dan baseert.

Universiteiten geven aan dat een goede toetsing van de achtergrond van nieuw personeel tijdsintensief is. Als toetsingsprocessen te lang duren bestaat het risico dat potentiële nieuwe werknemers voor een andere werkgever kiezen.

---

[31] Universiteiten 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.

Het opstellen van objectieve kaders en procedures vanuit de Rijksoverheid rondom screening zou volgens meerdere universiteiten dan ook wenselijk zijn. Immers zijn de sanctielijsten volgens meerdere universiteiten beperkt, niet volledig en/of niet beoordeeld door de EU, waardoor het voor universiteiten moeilijk is om toetsingsbeleid breder in te bedden in het wervingsproces. Bijvoorbeeld de ASPI-lijst wordt nu veel gebruikt, maar deze is ontwikkeld in Australië vanuit het oogpunt van Australische en Amerikaanse belangen.[32]

Wel geven universiteiten aan dat casussen erg van elkaar kunnen verschillen, dus dat er blijvend ruimte of autonomie moet zijn voor instellingen om - in het belang van goed wetenschappelijk onderzoek - een gemotiveerde uitzondering te kunnen maken op de kaders. Bijvoorbeeld wanneer universiteiten willen samenwerken met een risicovolle instelling, maar niet op een gevoelig onderwerp. Universiteiten geven aan dat sommige instituten die worden aangemerkt als (zeer) hoog risicovol vanuit het perspectief van kennisveiligheid, ook toonaangevend kunnen zijn in hun vakgebied.
Tegelijk zijn universiteiten bang dat autonomie rondom besluitvorming een (internationaal) waterbedeffect in de hand werkt. Studenten die bij de ene universiteit niet worden aangenomen, 'shoppen' mogelijk net zo lang bij andere universiteiten tot ze ergens wel worden aangenomen. Veel universiteiten hebben behoefte aan consistent en afgestemd Europees beleid op dit vlak, waar ze nu nog tegenstrijdige of verschillende richtlijnen per land zien.

Universiteiten vragen zich daarnaast af in hoeverre toetsing of screening van medewerkers voor specifieke vakgroepen zin heeft. Betrokkenen van in ieder geval twee universiteiten noemen dat medewerkers altijd contact zullen hebben met andere werknemers, bijvoorbeeld tijdens intervisiebijeenkomsten, tijdens informele gesprekken bij de koffieautomaat of via andere (sociale) relaties. Het risico op kennisdeling van vertrouwelijk materiaal bestaat daarmee volgens hen vrijwel altijd. Eén universiteit noemt als voorbeeld dat één van hun studenten die werkt met gevoelige data een relatie heeft met een Chinese medestudent.

Tot slot wijzen universiteiten op de incongruentie in toetsingsbeleid rondom masterstudenten en promovendi. Masterstudenten worden niet getoetst op hun achtergrond bij inschrijving aan de universiteit. Wanneer studenten na het afronden van hun master binnen dezelfde universiteit willen solliciteren op een promotieplaats kan er wel sprake zijn van een toetsingsprocedure naar de achtergrond van een student. Het is volgens universiteiten zeer lastig uit te leggen dat een masterstudent wordt afgewezen voor een PhD-positie omwille van de kennisveiligheid, terwijl hij of zij daarvoor al jaren aan diezelfde universiteit heeft gestudeerd.

6.2.3 Heimelijke beïnvloeding

Uit meerdere gesprekken halen we op dat universiteiten zich over het algemeen bewust zijn van het risico op heimelijke beïnvloeding, maar dat het fenomeen moeilijk is aan te tonen, concreet te maken of af te bakenen. Als gevolg is het niet goed aan te geven of risico's op heimelijke beïnvloeding worden over- of onderschat.

In ieder geval één universiteit geeft tot slot aan dat zicht krijgen op heimelijke beïnvloeding van de diaspora door statelijke actoren hoort bij de maatschappelijke opdracht van de veiligheidsdiensten, en niet bij die van de universiteit. Deze instelling vertrouwt er dan ook op dat de AIVD contact opneemt zodra het binnen de competenties van de universiteit valt om op een casus te acteren.

---

32 Home – Chinese Defence Universities Tracker — ASPI

6.3 Lessons learned

6.3.1 Toetsing achtergrond nieuwe kandidaten

Zowel uit de ingevulde vragenlijsten als de gespreksverslagen maken we op dat het toetsen van nieuwe en bestaande medewerkers op kennisveiligheidsrisico's zowel arbeidsintensief als juridisch gecompliceerd is. Universiteiten delen verschillende manieren waarop zij het toetsen toch op een wettelijk toegestane manier kunnen vormgeven. Om te voorkomen dat kandidaten bij voorbaat worden uitgesloten op basis van hun nationaliteit, geeft één universiteit aan voor het toetsen van nieuw personeel te kijken naar affiliaties in plaats van de afkomst.

6.3.2 Sollicitatiecommissie

Eén universiteit benoemt dat het een bewuste keuze is geweest om een facultaire sollicitatiecommissie samen te stellen met collega's uit verschillende landen. Hoofddoel van een diverse samenstelling is het voorkomen van *bias* richting sollicitanten. Daarnaast kan een commissielid goed inschatten welke universiteiten of kennisinstellingen uit (bijvoorbeeld) diens moederland wel en geen 'slechte naam' hebben. In potentie kan dit commissielid ook meedenken over de vraag welke kandidaten een mogelijk risico voor de kennisveiligheid zouden kunnen vormen en dus wel of niet zouden moeten worden uitgenodigd voor een sollicitatiegesprek. De betrokkene geeft tevens aan dat een divers samengestelde sollicitatiecommissie een belangrijke manier is om kandidaten het gevoel te geven dat hun achtergrond gerepresenteerd wordt binnen de selectiecommissie.

7 Conclusie en aandachtspunten

In dit hoofdstuk geven we een beknopte hoofdconclusie ten aanzien van het sectorbeeld kennisveiligheid universiteiten, namelijk dat het beleid nog in ontwikkeling is. Daarnaast concluderen we dat universiteiten tegen een aantal dilemma's aanlopen die van invloed zijn op de ontwikkeling van het kennisveiligheidsbeleid. Ten slotte presenteren we drie aandachtspunten voor de verdere ontwikkeling van het nationale kennisveiligheidsbeleid.

7.1 Conclusie: beleid in ontwikkeling

Het belang van het thema kennisveiligheid wordt gedragen door alle universiteiten. In ieder geval een kern van betrokkenen heeft zich het probleem eigen gemaakt, bij een deel van de instellingen en faculteiten is het al ingedaald op alle niveaus in de organisatie.
Vanaf 2022 is het kennisveiligheidsbeleid bij alle universiteiten in een stroomversnelling is geraakt, al waren verschillende universiteiten en faculteiten al langer bezig met onderdelen hiervan, bijvoorbeeld als gevolg van sanctieregelingen of door discussies over internationale partnerschappen met landen waar grondrechten niet worden gerespecteerd. Universiteiten zijn actief bezig om de adviezen van de Leidraad vorm te geven en hebben gehoor gegeven aan de oproep van de minister van OCW tot een risicoanalyse in 2022.

Het organisatorisch beleggen van verantwoordelijkheden en het ontwikkelen van beleid is verder gevorderd dan het vastleggen en uitvoeren van beleid in processen. Daarbij zijn er een aantal verschillen in de fase van beleidsvorming tussen onderdelen van de Leidraad, zoals Tabel 7.1 laat zien.

Tabel 7.1 Fase van ontwikkeling kennisveiligheidsbeleid universiteiten, naar onderdeel Leidraad (n=14[33]).

	Geen beleid	Beleid in ontwikkeling	Beleid is deels in ontwikkeling, deels vastgesteld en in uitvoering	Beleid is vastgesteld, uitvoering is aantoonbaar	Beleid kent deels een verbeter-cyclus	Er is een verbeter-cyclus aanwezig	Er is instellings-breed beleid met verbetercyclus
Risicoanalyse	0	9	1	3	1	0	0
Risicomanagement	0	9	2	2	1	0	0
Fysieke en digitale beschermings-maatregelen	0	2	3	7	0	0	1
Internationale partnerschappen	0	9	1	3	0	1	0
Juridische kaders	0	10	1	1	1	0	0
Personeelsbeleid	1	12	0	1	0	0	0

Beleid op fysieke en digitale bescherming is veelal vastgesteld en in uitvoering. Dit is ook beleid dat vaak al langer loopt dan de huidige aandacht voor kennisveiligheid. Het beleid op risicoanalyses en

[33] Bij fysieke en digitale beschermingsmaatregelen en juridische kaders hebben niet alle universiteiten zichzelf gescoord.

risicomanagement van internationale partnerschappen en de doorwerking van juridische kaders is meestal nog in ontwikkeling, en bij een aantal universiteiten al vastgesteld. De doorvertaling van kennisveiligheid naar personeelsbeleid is bij vrijwel alle universiteiten in ontwikkeling. Hier raakt het kennisveiligheidsbeleid individuele personen en collega's.

7.2 Dilemma's

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

7.2.1 Focus op technologisch onderzoek en proportionaliteit

Het kennisveiligheidsbeleid is in sterke mate gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie. De focus ligt daarmee op technologisch onderzoek. De relevantie en proportionaliteit van kennisveiligheidsbeleid is daarom punt van discussie voor met name de brede universiteiten. Zij ervaren hierop weinig richting en handvatten vanuit de overheid hoe onderzoek in de alfa- en gammawetenschappen zich dient te verhouden tot kennisveiligheid. Een aantal instellingen uit de zorg dat het beleid leidt tot een niet proportionele bureaucratie om risico's te beperken.

7.2.2 Academische waarden

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

7.2.3 Voorkomen stigmatisering en discriminatie

Universiteiten uiten zorgen over stigmatisering en discriminatie, of een cultuur van uitsluiting. Als het gaat over samenwerkingen met instellingen of onderzoekers uit specifieke landen ligt stigmatisering snel op de loer. Medewerkers in de kennisveiligheidsketen nemen soms het zekere voor het onzekere ("dan nemen we maar helemaal geen Russen of Iraniërs meer aan"), terwijl men het ook erover eens dat dit onwenselijk is. Abstract nationaal beleid vertaalt zich binnen de instellingen tot impact op het individuele niveau van veelbelovende sollicitanten en gewaardeerde collega's, wat betrokkenen binnen instellingen (onderzoekers, bestuurders en HR) in een lastige positie plaatst. Veel betrokkenen pleiten er daarom voor om altijd een inhoudelijke afweging te blijven maken op basis van meerdere factoren, waaronder specifieke affiliatie. Bovendien wil men voorkomen dat het risicovolle imago dat nu gekoppeld wordt aan bepaalde landen (zoals bijvoorbeeld China, Rusland of Iran) ervoor zorgt dat al het onderzoek (ook op niet-risicovolle kennisgebieden) met onderzoekers of instellingen uit dergelijke landen onmogelijk wordt, of dat alle onderzoekers uit die landen zich buitengesloten gaan voelen.

7.2.4 Kennisdilemma

Binnen universiteiten speelt een kennisdilemma. Onderzoekers zijn zelf het beste in staat om in te schatten of (samenwerkingen op) onderzoek veiligheidsrisico's met zich meebrengen. Zij hebben echter

minder kennis van formele exportregels of sanctiewetgeving. De mensen binnen de universiteit die dit wel hebben, zoals juridische afdelingen, export adviseurs en coördinatoren kennisveiligheid, missen vaak de inhoudelijke kennis om voor een specifieke samenwerkingsproject inhoudelijk te bepalen of er kennisveiligheidsrisico's aan zijn verbonden. Bij compliance met exportregels of het bepalen van andere mogelijke risico's ten aanzien van onderzoek of samenwerking, ligt de eerste signalerende verantwoordelijkheid daarom vaak bij de individuele onderzoeker. De institutionele afhankelijkheid van de individuele onderzoeker is kwetsbaar, dit benadrukt het belang van kennisveiligheidsbewustzijn onder onderzoekers.

7.2.5 Afbakening verantwoordelijkheden

Het kennisveiligheidsbeleid, de Leidraad en de voorbereidingen voor wetgeving rondom screening leiden tot discussies over de juiste afbakening van verantwoordelijkheden tussen universiteiten en de nationale overheid. Verschillende universiteiten geven aan dat de bescherming van de nationale veiligheid niet een taak moet worden van de universiteiten. Ook wordt de vraag opgeworpen wat een universiteit van zichzelf en een overheid van een universiteit mag verwachten. Veel betrokkenen geven aan dat ze niet naïef willen zijn, maar ook reëel zijn over wat een universiteit vermag tegenover gerichte inspanningen van statelijke actoren om bepaalde kennis te verzamelen.

De Nederlandse overheid legt op dit moment de verantwoordelijkheid voor specifieke beslissingen (met uitzondering van de screening van personeel voor risicovakgroepen in het kader van Missile Technology Control Regime) bij universiteiten. Dit vinden de meeste betrokkenen een goed uitgangspunt, omdat het een inhoudelijke genuanceerde afweging mogelijk maakt. Wel vragen universiteiten om middelen en informatiebronnen die hen in staat stellen om die verantwoordelijkheid te nemen. Dan gaat het bijvoorbeeld om informatie van veiligheidsdiensten via het Loket Kennisveiligheid, en objectieve kaders en procedures voor een zorgvuldige screening of toetsing van personen.

7.2.6 Gelijk speelveld

Ten slotte hebben veel universiteiten behoefte aan duidelijker nationaal en Europees beleid, inclusief duidelijke richtlijnen en tools vanuit het perspectief van de belangen en waarden van Europa. Daarbij benadrukken universiteiten ook het belang voor consistent en afgestemd nationaal en Europees beleid. Zij zien nu nog te vaak tegenstrijdige adviezen, waar een samenwerking met een buitenlandse universiteit of bedrijf door het ene overheidsinstituut wordt afgeraden, terwijl deze wordt gestimuleerd door een ander overheidsinstituut. Zeker waar onderzoek vaak in consortia wordt uitgevoerd en op basis van Europese financiering, zien onderzoekers verschillen in de richtlijnen die landen meegeven. Verschillende universiteiten vrezen een (inter)nationaal waterbedeffect, waarbij strenge richtlijnen op kennisveiligheid binnen de eigen instelling of het eigen land simpelweg ertoe leiden dat risicovolle samenwerkingen worden aangegaan door andere instellingen in Nederland of Europa. Het maken van EU-brede of internationale afspraken en het beschermen van de kansen voor goede wetenschap zijn van belang voor het concurrentievermogen van de Nederlandse wetenschap.

7.3 Aandachtpunten

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

Ten eerste gaat het dan om de **conceptualisering van kennisveiligheid** en gebruik van termen. Veel universiteiten volgen in hun beleid de Leidraad, maar juist instellingen die al verder zijn, hebben een aangepaste invulling gegeven aan wat zij wel en niet onder kennisveiligheid verstaan.
Daarnaast wordt in de praktijk op verschillende manieren invulling gegeven aan begrippen als samenwerking en partnerschappen, wat invloed heeft op het analyseren en mitigeren van risico's. Ook de afbakening van sensitieve kennis en technologie, dual-use toepassingen en kroonjuwelen van instellingen is nog niet volledig uitgekristalliseerd. Daarbij worden verschillende lijsten gehanteerd in diverse contexten. Het zou nuttig zijn om hier als overheid en sector gezamenlijk verder aan zowel conceptualisering als definiëring te werken, en dit te verwerken in een volgende editie van de Nationale Leidraad Kennisveiligheid. De AWTI geeft in haar rapport 'Kennis in conflict' eveneens dit aandachtspunt (Aanbeveling 1. Conceptualiseer: verbeter het begrip van kennisveiligheid).

Ten tweede, de Nederlandse overheid legt op dit moment veel **verantwoordelijkheid bij universiteiten**. Dit vinden de meeste betrokkenen een goed uitgangspunt, omdat het een inhoudelijke genuanceerde afweging mogelijk maakt. Wel vragen universiteiten om duidelijke (afwegings)kaders, middelen en informatiebronnen die hen in staat stellen om die verantwoordelijkheid te nemen. Dan gaat het bijvoorbeeld om informatie van veiligheidsdiensten via het Loket Kennisveiligheid, objectieve kaders en procedures voor een zorgvuldige achtergrondtoetsing van personen, en lijsten van risicovolle instellingen die actueel worden gehouden. Op dit moment zijn de risicoprofielen volgens meerdere universiteiten beperkt, niet volledig en niet beoordeeld door de EU, waardoor het moeilijk is om achtergrondtoetsing in te bedden in een werkbaar wervingsproces. Tegelijk erkennen gesprekspartners dat het moeilijk zal zijn om deze helderheid te geven. Bestaande kaders en lijsten worden ofwel te generiek bevonden, ofwel te lang en onoverzichtelijk. Onderliggend zien we een behoefte aan ruimte voor proportionaliteit in afwegingen voor de eigen situatie, maar ook de wens voor uniforme praktijken tussen universiteiten binnen Nederland en Europa. De AWTI geeft in haar rapport 'Kennis in conflict' eveneens dit aandachtspunt (Aanbeveling 2. Differentieer: in risico's, maatregelen en organisaties).

Ten derde zien we als aandachtspunt het belang van een **blijvende dialoog en onderling vertrouwen** tussen de overheid en de wo-sector. Er is waardering voor het Loket Kennisveiligheid en voor de verbindende rol van het ministerie van OCW. Tegelijkertijd zijn er zorgen dat beleidsontwikkelingen en verzoeken vanuit de overheid elkaar te snel opvolgen, waardoor beleidsontwikkeling minder nauwkeurig of genuanceerd uitgevoerd kan worden.

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[34]. 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.

34

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 de technology/knowledge transfer office(s) 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 startups. (Indien uw instelling niet beschikt over een technology/knowledge transfer office graag "n.v.t." invullen)
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.

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[35] 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.

35 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.

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?
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, 11 september 2023
In opdracht van het ministerie van OCW