VU VRIJE UNIVERSITEIT AMSTERDAM

Kader Kennisveiligheid VU

Opgesteld door de Adviesgroep Kennisveiligheid

Inleiding

Wetenschapsbeoefening is ondenkbaar zonder internationale samenwerking en Nederlandse kennisinstellingen hebben een goede reputatie in de wereld. Deze reputatie hangt samen met de hier aanwezige academische vrijheid, integriteit en openheid.

Naast kansen brengen internationale samenwerking ook risico's met zich mee. Er vinden geopolitieke machtsverschuivingen plaats, waarbij geopolitiek, veiligheid en economie met elkaar verweven zijn, en landen kennis en innovatie als machtsmiddel zien. Om internationale samenwerking zo veilig mogelijk te doen verlopen heeft de VU kennisveiligheidsbeleid ontwikkeld. De VU volgt bestaande wet- en regelgeving rondom samenwerking met internationale partners. De afgelopen periode is het bewustzijn gegroeid dat ook samenwerkingen, die volgens wet- en regelgeving zijn toegestaan, niet altijd wenselijk zijn. Ook hier wordt in het beleid aandacht aan besteed.

Dit document met het kader 'kennisveiligheid' is een belangrijke stap naar een bredere aanpak van kennisveiligheid op de VU. Het Kader Kennisveiligheid is gebaseerd op de Nationale Leidraad Kennisveiligheid. Het kader ondersteunt het gesprek over het onderwerp, de afweging en het besluit om wel of niet (verder) samen te werken met een persoon, instelling, financier of opdrachtgever. Voor het aangaan of verlengen van samenwerkingen is het verplicht de vragen van het kader te beantwoorden. Door systematisch de verschillende aspecten van de samenwerking langs te lopen en op veiligheidsrisico's te beoordelen kan een gefundeerd, traceerbaar en herhaalbaar besluit worden genomen over de samenwerking. Waarbij strategische overwegingen ook een rol kunnen spelen. Bij het opstellen van het kader is rekening gehouden met de verschillende wetenschappelijke disciplines die op de VU beoefend worden. Naast kennisveiligheid zijn ethische overwegingen ook belangrijk bij het besluit om wel of niet samen te werken. Binnen de VU wordt ook aan beleid op dit onderwerp gewerkt. Op het moment dat dit meer concreet wordt, zal bekeken worden hoe kennisveiligheid en overwegingen vanuit andere perspectieven op elkaar afgestemd kunnen worden. Het Kader Kennisveiligheid kan als aanvulling gebruikt worden op al bestaande processen rondom samenwerkingen binnen faculteiten.

Rondom het proces, besluitvorming, en ondersteuning van het kader zijn keuzes gemaakt in overleg met faculteiten, het programma kennisveiligheid en het CvB. Deze keuzes worden toegelicht in 2.2. Het kader is vastgesteld door het College van Bestuur en treedt in werking vanaf 1 september 2023. Het geldt voor iedere persoon, faculteit, dienst en instituut verbonden aan de VU Amsterdam. De vragen van het kader, zoals in 2.2 staan, zullen dan eerst beantwoord moeten worden voordat er verder gesproken kan worden over het aangaan of verlengen van een samenwerking.

Op de VU is de Adviesgroep Kennisveiligheid door het CvB ingesteld voor het ontwikkelen van beleid en het geven van advies. De adviesgroep rapporteert aan de Rector. De eerste uitwerking van het beleid staat beschreven in dit document. Sectie 1 beschrijft kort wat kennisveiligheid is en in sectie 2 staat de wijze waarop de VU kennisveiligheid heeft geïmplementeerd. Het beoogde kennisveiligheidsproces, uitgewerkt in sectie 2, is nog geen staande praktijk en verschillende acties zijn nodig om tot deze situatie te komen. Deze staan op hoofdlijnen beschreven in sectie 3, waarin de onderwerpen en ontwikkelingen staan, die de komende periode aandacht nodig hebben binnen de VU in samenwerking tussen de faculteiten en diensten. Hierbij is het doel om zo veel mogelijk tot integrale processen en een verder uitgewerkt beleid te komen. Bijvoorbeeld door te streven naar een portal waar alle informatie en stappen, die voor een samenwerking nodig zijn, bij elkaar staan. In voorbereiding staat informatie over kennisveiligheid op vu.nl. Dit kader wordt geactualiseerd wanneer omstandigheden daarom vragen.

1. Kennisveiligheid

Goed hoger onderwijs en wetenschap kunnen niet zonder internationale samenwerking en wetenschappelijk talent van over de hele wereld. Kennisveiligheid is erop gericht dat internationale samenwerking met zo min mogelijk risico's kan plaatsvinden.

Het gaat daarbij om het (her)kennen van veiligheidsrisico's rondom internationale samenwerking met als doel om gewenste internationale wetenschapssamenwerking zo veilig mogelijk te laten plaatsvinden. Aan de basis staan de kernwaarden 'academische vrijheid' en 'wetenschappelijke integriteit'.

Kennisveiligheid is gericht op drie facetten. Allereerst gaat het om het voorkomen van ongewenste overdracht van sensitieve[1] kennis en technologie. Overdracht is ongewenst als deze de nationale veiligheid aantast, bijvoorbeeld vanwege militaire toepassing van de onderzoeksresultaten. Hiervoor is wet- en regelgeving van de nationale overheid van toepassing. Daarnaast gaat kennisveiligheid om het voorkomen van heimelijke beïnvloeding van onderzoek en onderwijs door statelijke actoren. Deze inmenging brengt onder meer de academische vrijheid en de sociale veiligheid in gevaar. Als derde gaat kennisveiligheid ook over ethische kwesties die kunnen spelen in de samenwerking met landen die grondrechten niet respecteren. Voor de laatste twee onderdelen moet van geval tot geval bekeken worden wat risico's en kansen van een samenwerking zijn. Hierbij is het de ambitie om een cultuur te stimuleren waar VU-medewerkers met elkaar in gesprek gaan over de wenselijkheid van samenwerkingen en het voorkomen van ongewenst gebruik van VU-onderzoek, kennis of technologie.

De VU herkent en onderschrijft de mogelijke risico's van internationale samenwerking en wil deze op een gebalanceerde wijze beperken met oog voor ongewenste effecten. Hiervoor is een aanpak opgesteld die de risico's en de kansen van samenwerkingen in beeld brengt en ruimte biedt voor maatwerk. Hiermee willen we voorkomen dat er gestigmatiseerd of gediscrimineerd wordt, dat door stringente regels samenwerking met bepaalde landen onmogelijk wordt waar het juridisch wel mag, of dat de concurrentiepositie van de universiteit verzwakt. Dit is niet eenvoudig en zal bij het in praktijk brengen ongetwijfeld soms schuren. Beoogd is een heldere aanpak die wendbaar en goed toepasbaar is, zodat onderzoekers en vakgroepen snel weten of een samenwerking aangegaan kan worden of – als dat niet het geval is – waarom niet. Kennisveiligheid is geen statisch gegeven. Zo hebben veranderende geopolitieke verhoudingen invloed op hoe naar (lopende) samenwerkingen wordt gekeken. Vanuit de overheid en maatschappij wordt druk uitgevoerd op de hoger onderwijsinstellingen om meer aandacht te besteden aan kennisveiligheid en in de toekomst kan dit tot verdere ontwikkelingen leiden.

1 Zie vraag 4 van het kader voor meer informatie

2. Implementatie kennisveiligheid op de VU

Kennisveiligheidsbeleid heeft impact op de hele universiteit en is daarmee een gedeelde verantwoordelijkheid binnen de universiteit. Internationale samenwerking start vaak bij enthousiaste wetenschappers op informele basis. Deze samenwerking kan groeien tot iets groters, waar meer wetenschappers, vakgroepen en zelfs instellingen bij worden betrokken en daarmee een formeel karakter krijgt.

Het kennisveiligheidsbeleid van de VU is laagdrempelig en biedt handvatten om mogelijke risico's in onderzoek, onderwijs en bedrijfsvoering in kaart te brengen en daarop te reageren. Het is een uitwerking van de vraag of het (voorgenomen) onderzoek potentieel ongewenst of onethisch kan worden ingezet en/of onze nationale veiligheid kan raken, zodat vervolgens advies gegeven kan worden over het uitvoeren van dit onderzoek en erover besloten wordt.

2.1 VU Kader Kennisveiligheid

In UNL-verband wordt nauw samengewerkt om tools te ontwikkelen, die onderzoekers en ondersteuners (zoals contractmanagers en kennisveiligheidsadviseurs) kunnen helpen bij het aangaan, uitvoeren en evalueren van internationale samenwerkingen.

De tools omvatten handreikingen voor alle fasen van een samenwerking: van een onderzoek naar- en de selectie van een partner (fase 1), de onderhandelingen (fase 2), de daadwerkelijke samenwerking (fase 3) tot aan de evaluatie (fase 4). Deze zijn beschikbaar via vu.nl (kennisveiligheid).

De vragen en aandachtspunten vanuit kennisveiligheid bij de VU zijn uitgewerkt in zeven stappen. Faculteiten kunnen waar nodig aanvullende vragen en informatie toevoegen bij gebruik in de betreffende faculteit, bijvoorbeeld vanuit een ethische code voor onderzoek. Hoewel de focus van het kader onderzoek is, biedt het kader ook 'stappen' voor diensten en faculteiten, voor bijvoorbeeld het aannemen van OBP.

Wettelijk kader – Is het juridisch toegestaan?

1. Staat de persoon, het bedrijf, de organisatie of het land met wie we willen samenwerken op de EU of VN-sanctielijst?

Samenwerken met personen, bedrijven, organisaties of landen die voorkomen op de EU- en VN-sanctielijst is strafbaar en dus niet toegestaan. Ook kunnen bepaalde technologieën in relatie tot bepaalde landen onder sancties vallen. Screen CV's van personen op (indirecte) affiliaties met organisaties die voorkomen op de EU- en VN-sanctielijst. Zie: EU Sanctions Map. Als de persoon in de afgelopen 4 jaar verbonden is geweest met een gesanctioneerde organisatie, bespreek dit met de HR-adviseur en/of leidinggevende.

2. Valt het onderzoek onder de Dual-use Verordening?

Als sprake is van een onderzoek dat betrekking heeft op dual-use producten, programmatuur of technologie, dan mag dit onderzoek alleen worden uitgevoerd met een vergunning van de Centrale Dienst voor In- en Uitvoer (CDIU) van de Douane. De volgende vragen zijn hierbij van belang:

a. Dual-use?

- Is sprake van (kennis over) producten, programmatuur of technologie, die zowel een civiele als een militaire bestemming kunnen hebben (met inbegrip van alle (kennis over) producten die kunnen worden gebruikt voor het ontwerp, de ontwikkeling, de productie of het gebruik van nucleaire, chemische of biologische wapens of hun overbrengingsmiddelen)?
- Zo ja, ga verder naar vraag 2b.
- Zo nee, dan is de Dual-use Verordening niet van toepassing en ga verder naar vraag 3.

Let op, in bijlage 1 van de Dual-use Verordening staat wat **in ieder geval** wordt beschouwd als dual-use producten, programmatuur en technologie.

b. Fundamenteel wetenschappelijk onderzoek?

- Is sprake van *fundamenteel* wetenschappelijk onderzoek?
- Fundamenteel wetenschappelijk onderzoek = experimenteel of theoretisch werk dat hoofdzakelijk wordt gedaan om nieuwe kennis te verkrijgen over de fundamentele beginselen van verschijnselen of waarneembare feiten, en dat in eerste instantie **niet** is gericht op een bepaald praktisch doel of oogmerk.
- Zo ja, dan is geen vergunning vereist, ga verder naar vraag 3.
- Zo nee, ga naar vraag 2c.

Let op, hoe hoger het Technology Readiness Level (TRL) hoe minder snel mag worden aangenomen dat sprake is van fundamenteel wetenschappelijk onderzoek.

c. Voor iedereen beschikbaar?

- Is sprake van (kennis over) producten, programmatuur of technologie die voor iedereen beschikbaar is? Voor iedereen beschikbaar = producten, technologie of programmatuur die voor iedereen zonder beperkingen aan de verdere verspreiding daarvan beschikbaar zijn gesteld.
- Zo ja, dan is geen vergunning vereist, ga verder naar vraag 3.
- Zo nee, dan is zeer waarschijnlijk een vergunning vereist. Neem contact op met Bestuurlijke en Juridische Zaken via kennisveiligheid@vu.nl

Let op, van voor iedereen beschikbare producten, technologie of programmatuur is geen sprake als de kennis vóór het onderzoek nog niet beschikbaar is. Het feit dat *uiteindelijk* openbaar zal worden gepubliceerd over de uitkomsten van dit onderzoek betekent dus **niet** dat al sprake is van (kennis over) producten, programmatuur of technologie die voor iedereen beschikbaar is.

Bij vragen of twijfel neem contact op met Bestuurlijke en Juridische Zaken via kennisveiligheid@vu.nl

Risicobeheersing – Welke risico's zijn er?

3. Is de partner verbonden (geweest) aan een militaire organisatie buiten de EU?
Samenwerking met militaire organisaties en daaraan gelieerde instellingen van landen buiten de EU is zeer ongewenst. Screen CV's van personen op (indirecte) affiliaties. Als de persoon in de afgelopen 4 jaar verbonden is geweest met een van deze instellingen, anders dan als BSc of MSc student, dan is het uitgangspunt dat de samenwerking niet kan doorgaan. De ASPI unitracker geeft overzicht van universiteiten en hun relaties met het Chinese leger. Onder *military* en *national defence* staan universiteiten waarmee samenwerking zeer ongewenst is. Voor de vier kwalificaties staan de uitgangspunten hieronder, afwijken mag alleen met goedkeuring van de tekenbevoegde:

- **Very High Risk** – samenwerking is zeer ongewenst
- **High risk** – vermijd dual-use onderzoek, houd afstand van defensie gerelateerde onderzoeksafdelingen, vermijd sensitieve onderzoeksgebieden
- **Medium risk** – houd afstand van defensie gerelateerde onderzoeksafdelingen, vermijd sensitieve onderzoeksgebieden
- **Low Risk** – vermijd sensitieve onderzoeksgebieden

4. Bevat de samenwerking sensitief onderzoek?
Het gaat om sleuteltechnologieën[2] en Emerging Technologies[3], dit zijn technologieën die door de Nederlandse overheid als militair, economisch en geopolitiek strategisch worden gezien. Samenwerking met risico landen[4] hierop is doorgaans ongewenst. Heeft de samenwerking betrekking op een sensitief kennisgebied met een partner uit een land met een verhoogd risicoprofiel (dit zijn landen die op de EU sanctielijst staan en zie het dreigingsbeeld)? Maatwerk is in deze gevallen nodig en het advies is om de Adviesgroep Kennisveiligheid in te schakelen via kennisveiligheid@vu.nl. In sommige gevallen kan de conclusie zijn dat samenwerking niet mogelijk is, ook niet met een goed contract. Dat is het geval wanneer de restrisico's niet acceptabel zijn voor de verantwoordelijke risico-eigenaar (de Dienst, Faculteit of het College van Bestuur).

5. Is sprake van mogelijk ethische onverantwoorde praktijken of vraagstellingen?
Denk aan het risico op schending van mensenrechten of van academische waarden, misbruik van kennis, veiligheid van onderzoekers en respondenten waaronder kans op druk en dwang, onbedoelde kennisoverdracht, of aan schade toebrengen aan mensen, dieren of het milieu. Bij een landenscore van 0.4 of lager op de Academic Freedom Index[5] moet de samenwerking worden besproken met de hiërarchisch beslissingsbevoegde leidinggevende (directeur bedrijfsvoering of directeur dienst, mogelijk gedelegeerd naar een contactpersoon bij het organisatieonderdeel).

6. Is sprake van eenzijdige externe financiering bij de samenwerking of bij inkomende medewerkers?
Doe aan due diligence (zie vu.nl). Stel jezelf ook de vragen wat mogelijke redenen voor de partner zijn om het onderzoek of persoon te financieren en wat de mogelijke risico's van deze eenzijdige financiering zijn. Hieronder vallen ook onderzoekers die uit eigen middelen de kosten financieren. Voor landen die lager scoren dan 0.4 op de Academic Freedom Index is de VU terughoudend bij de aanstelling van onderzoekers, hierbij gelden de volgende beperkingen:

- Geen bursalen die korter dan twee jaar naar de VU komen en begeleid worden vanuit het thuisland
- Geen onderzoekers op dual-use en sensitieve onderzoeksgebieden
- Geen onderzoekers afkomstig van een partner die valt onder de randvoorwaarden voor Very High Risk van vraag 3

Wel bursalen door de VU geselecteerd op een onderwerp dat door de VU is aangedragen, en een promotie op de VU.

2 Sleuteltechnologieën: de verwachting is dat hier een toetsingskader voor wordt opgesteld door de overheid. Een overzicht van sleuteltechnologieën staat in bijlage 1.
3 Emerging technologies: hiervoor komt een VU-webpagina beschikbaar in 2023.
4 Risicovolle landen: dit zijn landen die laag scoren op de Academic Freedom Index, respect voor de rechtstaat, waar nodig aangevuld met informatie uit het dreigingsbeeld opgesteld door de AIVD.
5 In de toekomst wordt dit mogelijk uitgebreid met ethische overwegingen over de samenwerking met een partner. Faculteiten kunnen relevante informatie bij deze vraag gebruiken, die bijvoorbeeld al gebruikt wordt bij de beoordeling door de facultaire ethische commissie.

Geen belemmering – De samenwerking kan aangegaan worden

7. Er zijn geen belemmeringen voor samenwerking
Evenwel is het raadzaam om de Partnering Tools te bekijken als je een internationale samenwerking start. Daarin staan tips voor alle fasen van samenwerken: kennismaken, contracteren, uitvoeren en evalueren. Daarnaast is de due diligence pagina relevant om te bekijken, deze zijn beschikbaar op vu.nl.

2.2 Toelichting kader

Het VU Kader Kennisveiligheid, zoals hierboven weergegeven, biedt medewerkers inzicht in de mogelijke kennisveiligheidsrisico's van een beoogde samenwerking in onderzoek. Het is gericht op samenwerkingen, waarbij contracten gesloten worden tussen de VU en een andere instelling, financier, opdrachtgever, of waarbij individuen een relatie aangaan met de VU (bijvoorbeeld: gastvrijheid, buitenpromovendi, toetreden tot een graduate school). De vragenlijst is een basischecklist en moet worden ingevuld voor alle projecten. Als alle vragen met 'nee' worden beantwoord, is geen verdere actie nodig. Dit zal bij veel projecten de situatie zijn.

De eerste twee vragen van het kader zijn gerelateerd aan wet- en regelgeving. Indien de eerste vraag met 'ja' wordt beantwoord, is samenwerking niet mogelijk. Als de tweede vraag met 'ja' wordt beantwoord, dan moet bekeken worden of een exportvergunning aangevraagd wordt. Neem hiervoor contact op met kennisveiligheid@vu.nl.

Vragen drie t/m zes zijn gericht op samenwerkingen die wettelijk gezien plaats mogen vinden, maar waar de VU vanuit kennisveiligheid nader onderzoek nodig vindt. Indien één van deze vragen met 'ja' wordt beantwoord, zijn er mogelijke risico's in de samenwerking. In dat geval of als er onduidelijkheden zijn, informeert de VU-medewerker de leidinggevende en de hiërarchisch beslissingsbevoegde leidinggevende (directeur bedrijfsvoering of directeur dienst). De directeur kan hiervoor een contactpersoon kennisveiligheid instellen, de faculteiten en diensten besluiten voor zichzelf hoe het proces ingericht wordt. De beslissingsbevoegd leidinggevende of de contactpersoon kennisveiligheid bespreekt de initiële risico-inschatting met de medewerker. Vervolgens wordt een risicomanagementproces aan de hand van een uitgebreidere vragenlijst doorlopen (zie bijlage 2), gericht op het identificeren en inschatten van risico's. Deze ingevulde vragenlijst wordt bewaard, zodat deze als nodig geraadpleegd kan worden. Daarbij is ook aandacht voor de kans van optreden van het onbedoelde effect, de grootte van de impact en welke maatregelen kunnen worden getroffen om het risico te verkleinen. Ook de kansen worden besproken die de samenwerking de VU brengt.

Indien er in de faculteit/dienst een contactpersoon kennisveiligheid aanwezig is, geeft deze een onderbouwd advies aan de beslissingsbevoegd leidinggevende (directeur bedrijfsvoering of directeur dienst). De directeur kan volgens de in de procuratieregeling (vastgesteld in januari 2021) gestelde grenzen besluiten nemen over samenwerkingen of het CvB vragen een besluit te nemen. De faculteit of dienst monitort de risico's gedurende de samenwerking indien deze doorgang vindt.

Bij twijfel kan de directeur bedrijfsvoering, dienstdirecteur of het CvB, de Adviesgroep Kennisveiligheid om advies vragen. Het uiteindelijke besluit wordt door de adviesvrager genomen. De Adviesgroep Kennisveiligheid wordt tijdig door de adviesvrager geïnformeerd als het uiteindelijke besluit van de faculteit zal afwijken van het advies van de adviesgroep. Indien nodig kan de Adviesgroep Kennisveiligheid advies inwinnen bij het Nationaal Loket Kennisveiligheid en dit advies gebruiken in het advies naar de adviesvrager. Houd rekening met een doorlooptijd aangezien het landelijk loket gemiddeld 15 werkdagen aanhoudt voor het geven van een advies.

In geval er een mogelijk incident is rondom kennisveiligheid, dan informeert de betrokken onderzoeker de directeur bedrijfsvoering, die vervolgens de adviesgroep op de hoogte brengt. Als gewenst kan de adviesgroep ondersteunen bij het onderzoeken van het incident en het treffen van maatregelen. Voordat de conclusie van het incident wordt vastgesteld en mogelijke vervolgacties bepaald zijn, wordt de Adviesgroep Kennisveiligheid geconsulteerd.

3. Vervolgstappen

Het is de verwachting dat bij de introductie van het kader veel vragen komen van medewerkers, faculteiten en diensten. Door voorbeelden van onderzoek op gevoelige onderwerpen bij faculteiten verder uit te werken, wordt ervaring opgedaan met dit kader en zal het waar nodig worden aangepast. De VU onderneemt de nodige acties om de beoogde situatie zoals beschreven in sectie 2 te bereiken.

Risicomanagement: de VU werkt aan een dialoog over kennisveiligheid om een cultuur te bewerkstelligen waarin er met elkaar hierover gesproken wordt. Daarnaast wordt een risicomanagementproces opgesteld en wordt verkend of het wenselijk is om kennisveiligheid op te nemen in de planning & control cyclus van diensten en faculteiten naar CvB en van CvB naar RvT. Daarnaast moet uitgewerkt worden op welke wijze de aanvullende vragenlijsten bewaard worden, zodat deze op een later moment geraadpleegd kunnen worden. Om ervan te leren, of in geval van een incident.

Verbinden van structuren en instellen aanspreekpunt binnen faculteiten/diensten: Overlegstructuur opzetten tussen de Adviesgroep Kennisveiligheid en de stuurgroep risicomanagement, en een contactpersoon kennisveiligheid bij faculteiten en diensten aanstellen. Dit kan ook de directeur bedrijfsvoering of directeur dienst zijn. Voor vragen kan contact opgenomen worden met kennisveiligheid@vu.nl.

Informatievoorziening, bewustwording en training. Veel VU-medewerkers hebben al van kennisveiligheid gehoord, maar weten nog niet precies wat het inhoudt en wat voor impact het op hun werk gaat hebben. Daarom zorgt de VU ervoor dat het beleid rondom kennisveiligheid gemakkelijk is te vinden op de VU-website. Daarnaast zal de VU een campagne opzetten om het onderwerp beter bekend te maken op de universiteit en zullen trainingen aangeboden worden aan de medewerkers.

Afstemmen met ander VU-beleid en lijnorganisatie. Verschillende onderdelen van kennisveiligheid passen bij werkzaamheden en verantwoordelijkheden van de lijnorganisatie. Deze onderdelen staan ook omschreven in de Nationale Leidraad Kennisveiligheid van de rijksoverheid. Met betrokkenen moet worden besproken op welke wijze kennisveiligheid onderdeel wordt van de werkzaamheden en welke onderdelen onder nieuwe functies en structuren vallen. Bijvoorbeeld met Ethische commissies, HR-medewerkers, IT, International Office, IXA-GO.

Bijlage 1 Overzicht van Sleuteltechnologieën

Het overzicht van de sleuteltechnologieën is te vinden op de kennisveiligheid pagina op vu.nl onder 'VU Kader Kennisveiligheid'. In verband met landelijke ontwikkelingen zal deze lijst aan verandering onderhevig zijn en is de actuele lijst online te raadplegen. Het is raadzaam om, voor het beoordelen of er sprake is van een sleuteltechnologie, altijd de meest actuele lijst op vu.nl te raadplegen. Zie voor meer achtergrondinformatie de NWO pagina Sleuteltechnologieën.

Bijlage 2: uitgebreide vragenlijst Kennisveiligheid

Voordat u de onderstaande vragen invult, vragen wij u of u aan kunt geven op welke van de 6 vragen u ja heeft geantwoord of bij welke vraag u twijfels bij had.

Vraag	Antwoord
1. Staat de persoon, het bedrijf, de organisatie of het land met wie we willen samenwerken de EU of VN-sanctielijst?	
2. Valt het onderzoek onder Dual-use Verordening?	
3. Is de partner verbonden (geweest) aan een militaire organisatie buiten de EU?	
4. Bevat de samenwerking sensitief onderzoek?	
5. Is sprake mogelijk ethische onverantwoorde praktijken of vraagstellingen?	
6. Is er sprake van eenzijdige externe financiering bij de samenwerking of bij inkomende medewerkers?	

In de onderstaande tabel staan aanvullende vragen over uw onderzoek en/of samenwerking. Deze vragen dienen beantwoord te worden indien u bij vraag 1 tot en met 6 van het VU Kader Kennisveiligheid één of meerdere keren ja heeft beantwoord, of als u twijfels heeft bij de beantwoording van een van deze vragen. Het invullen van deze aanvullende vragen helpt ons, de VU Adviesgroep Kennisveiligheid, om uw adviesverzoek zo goed mogelijk te kunnen behandelen en beantwoorden.

Vraag over de samenwerking	Antwoord[6]
Contactpersoon	
Leidinggevende van indiener	
Naam van de samenwerking of project	
Tot wanneer loopt de samenwerking? (Maand en jaar)	
Faculteit van de VU	
Afdeling	
Om welk onderzoeksgebied gaat het?	

Met welke instelling/organisatie is de samenwerking? Mocht het alleen een kandidaat (of meerdere) betreffen, geef dan de instelling/organisatie aan waar de kandidaat van afkomstig is. Graag ook het land van de instelling/organisatie vermelden i.v.m. mogelijke sancties.	
Beschrijf in drie regels het onderwerp van de samenwerking	
Wat is het belang van de samenwerking voor de VU? (Wat levert het de VU op wat anders niet mogelijk is?)	
Wat is het belang voor de onderzoeker en onderzoeksgroep?	
Valt het onderzoek in de categorie gevoelige onderzoeksgebieden? Geef een korte beschrijving van het onderzoek met aandacht in hoeverre de sleuteltechnologieën, emerging technologies, kroonjuwelen van de afdeling (zie uitleg[7] onderaan de tabel) wel of niet van toepassing zijn op het onderzoek, en wat de toepassing is.	
Zouden de onderzoeksresultaten en/of data gebruikt kunnen worden voor andere (onethische) doeleinden? Denk aan vragen als: (1) Kunnen de onderzoeksresultaten schade toebrengen aan mensen, dieren of het milieu (al dan niet na modificatie of versterking)? (2) Kunnen de onderzoeksresultaten leiden tot een schending van de mensenrechten? (3) Wat kan er gebeuren indien de onderzoeksresultaten en/of data in de verkeerde handen terecht komen?	
Wie zijn de samenwerkingspartners en wat voor soort samenwerking betreft het? Denk aan project uitwisseling studenten/ WP, kennisnetwerk, joint research, etc. Beschrijf het soort overeenkomst.	
Is een samenwerkingspartner verbonden aan een militaire organisatie buiten de EU? Vinden wij de partnerinstelling betrouwbaar of is deze betrokken bij de ontwikkeling van technologie die mogelijk gebruikt kan worden voor mensenrechtenschendingen of militaire technologie? Voor China zie: ASPI Unitracker. Dit is een lijst van Chinese universiteiten en hun relaties met het Chinese leger. Deze lijst bevat niet alleen informatie over de instituten, maar ook over specifieke labs binnen deze instituten. Houd er rekening mee dat een instituut zelf een gemiddeld risico kan zijn, maar een specifiek lab binnen dit instituut een hoog risico kan opleveren.	
Is op basis van de beschikbare bronnen voor de eventuele partneronderzoeker en partnerinstelling na te gaan of bepaalde alarmbellen afgaan? Bijvoorbeeld op het vlak mensenrechten, onderzoek, verbondenheid met een militaire overheid.	
Spelen ethische of morele dilemma's bij de samenwerking? Zo ja, geef een korte beschrijving? Denk aan schending van mensenrechten of van academische waarden, misbruik van kennis, veiligheid van onderzoekers waaronder de kans op druk en dwang, of onbedoelde kennisoverdracht (diversion).	

Is sprake van eenzijdige externe financiering bij de samenwerking of bij inkomende medewerkers? Stel jezelf ook de vragen wat mogelijke redenen voor de partner zijn om het onderzoek of persoon te financieren en wat de mogelijke risico's van deze eenzijdige financiering zijn. Hieronder vallen ook onderzoekers die uit eigen middelen de kosten financieren.	
Heeft de onderzoekspartner toegang tot de digitale of fysieke onderzoeksomgeving van de VU? Zo ja, gelden er beperkingen?	
Indien gebruik wordt gemaakt van een VU Laboratorium: beschrijf kort het type laboratorium en de te gebruiken technieken. Vermeld hierbij of er toegang is tot andere onderzoeken of opstellingen in het lab, en of deze (mogelijk) sensitief zijn.	
Welke (andere) risico's zijn verbonden aan de samenwerking?	
Welke acties zijn genomen om de risico's te beperken? Denk aan beperkte toegang tot bepaalde gebouwen of afdelingen, beperkte toegang tot online omgevingen en informatie.	
Zijn er nog zaken die je wilt benoemen, die in de vragenlijst nog niet aan de orde zijn gekomen? Vul die hier in.	
Waarom wegen de voordelen van de samenwerking zwaarder dan de risico's? Besteed aandacht aan: 1) wat de samenwerking de VU oplevert; 2) de risico's die aanwezig zijn bij de samenwerking; 3) de gevolgen van het beëindigen van de samenwerking intern (onderzoek, onderwijs, etc.) en extern (betrekking met partners, reputatie, ontbinden van contract, etc.).	

Uitkomst bespreking

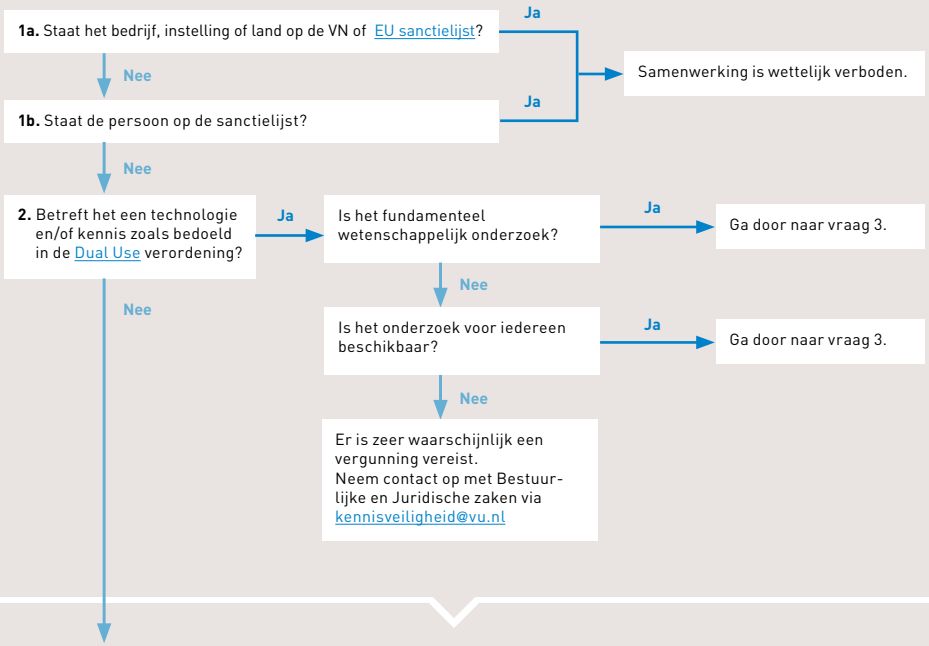
6 Al bekende informatie over de samenwerking is ingevuld. U kunt hier aanvullingen en aanpassingen op maken waar dat nodig is.
7 Uitleg sleuteltechnologieën, emerging technologies, kroonjuwelen.
Zie hiervoor bijlage 1. en zie TNO Rapport Herijking Sleuteltechnologieën 2023 voor het volledige rapport.

Bijlage 3

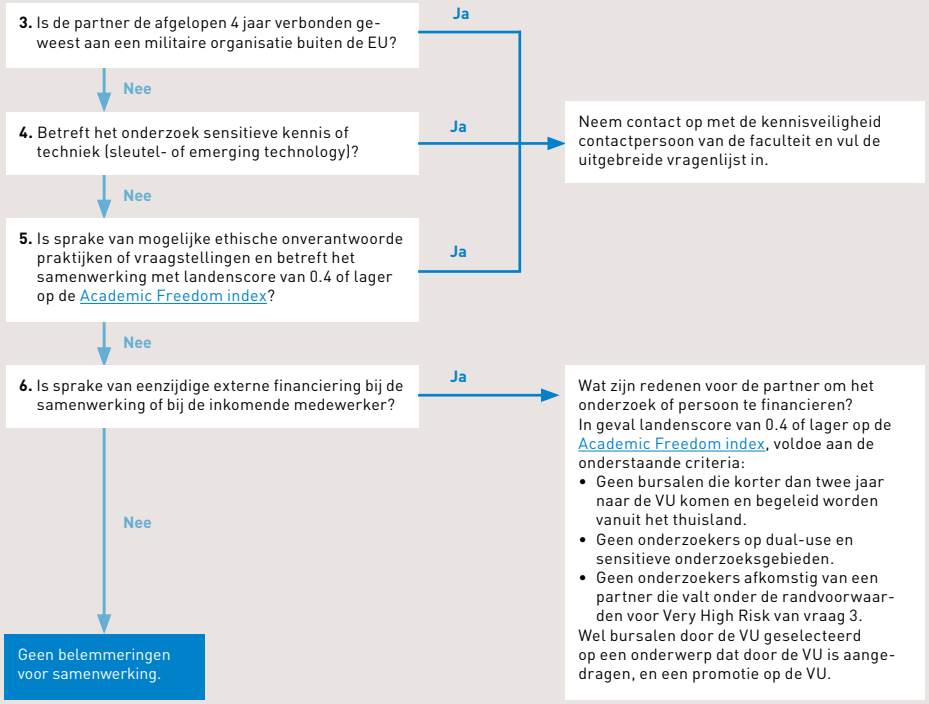
Is samenwerking met een instelling of persoon toegestaan en wenselijk?

Beantwoord de onderstaande vragen. **Als alle onderstaande vragen met 'nee' worden beantwoord dan zijn er geen belemmeringen.**
Het is dan evengoed raadzaam de Partnering Tools te raadplegen.

Wettelijk kader



Risico beheersing



Colofon
Het Kader Kennisveiligheid VU is opgesteld door de Adviesgroep Kennisveiligheid. Meer informatie over kennisveiligheid en het VU-beleid hiervoor is te vinden op de medewerkerspagina kennisveiligheid.

Contact opnemen met de adviesgroep kan via kennisveiligheid@vu.nl. Op de medewerkerspagina kennisveiligheid staan de *facultaire contactpersonen kennisveiligheid*. De facultaire contactpersonen zijn in de regel het eerste aanspreekpunt.

Vormgeving
Haagsblauw i.o.v. VU Designstudio

Fotografie
Peter Valckx

Versie 1.0: 18 juli 2023
2073402


VU
VRIJE
UNIVERSITEIT
AMSTERDAM