

Kennisveiligheid

Facultaire procedure en samenvatting VU Kader
Kennisveiligheid voor internationale samenwerking

Over dit document

<i>URL</i>	Kennisveiligheid
<i>status</i>	Facultaire procedure
<i>versie</i>	3
<i>auteurs</i>	Esther van de Hengel, Maaïke Verbree, Kirsty Brachel
<i>datum</i>	28 november 2023
<i>verspreiding</i>	Faculteit

Vastgestelde versies

#	Date	Auteur(s)	Changes
1	20220706	Esther van den Hengel, Maaïke Verbree	
2	FB-besluit 20231103	Kirsty Brachel, Maaïke Verbree, Esther van den Hengel	Aansluiting op VU Framework Knowledge Security
3	FB-besluit20231103-v3	Kirsty Brachel	Aanpassing links vanwege vernieuwing o.a. factsheets

Inhoud

FACULTAIRE PROCEDURE	2
KADER KENNISVEILIGHEID	3
Wettelijk kader: Is het juridisch toegestaan?	4
Risicobeheersing: Welke risico's zijn er?	4
ADDITIONELE INFORMATIE	5
Contacten	5
Pagina's	6

Achtergrond

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

Kennisveiligheidsbeleid heeft drie doelen:

1. Allereerst gaat het om het voorkomen van ongewenste overdracht van sensitieve kennis en technologie. Overdracht is ongewenst als deze de nationale veiligheid aantast.
2. Daarnaast gaat kennisveiligheid om heimelijke beïnvloeding van onderwijs en onderzoek door statelijke actoren. Deze inmenging brengt de academische vrijheid en de sociale veiligheid in gevaar.
3. Tot slot gaat kennisveiligheid over ethische kwesties die kunnen spelen in de samenwerking met landen die grondrechten niet respecteren en/of, in het geval van de VU, instituten die onze academische waarden niet delen.

Het [VU Kader Kennisveiligheid](#) is op 1 september 2023 inwerking getreden. Met dit kader wordt gewaarborgd dat internationale samenwerking kan plaatsvinden op een veilige manier. Het ondersteunt de afweging om wel of niet een samenwerking met een persoon, instelling, financier of opdrachtgever aan te gaan. Dat betekent dat bij het aangaan van internationale samenwerking en/of relaties voor onderzoek, onderwijs en bedrijfsvoering iedereen altijd de vragen uit dit kader moet beantwoorden voordat een samenwerking kan worden aangegaan.

Een belangrijk aandachtspunt is het vergroten van de bewustwording van alle VU-medewerkers op het gebied van kennisveiligheid. Deze facultaire procedure over kennisveiligheid beoogt daaraan bij te dragen.

Facultaire procedure

Voor medewerkers van de Faculteit der Bètawetenschappen (BETA) zijn de volgende processtappen leidend bij de juridische toetsing en risicoafweging van kennisveiligheid bij het aangaan van internationale samenwerking:

1. Als een medewerker een internationale samenwerking wil aangaan of verlengen, dan moeten vóóraf de 6 vragen van het [Kader Kennisveiligheid](#) worden beantwoord.
 - a. Indien het gaat om de werving van een nieuwe medewerker¹ of verlenen van gastvrijheid, dan moet de HR-adviseur² worden geïnformeerd. De HR-adviseur heeft een adviserende en signalerende rol met betrekking tot Kennisveiligheid en kan een medewerker adviseren de vragen van het Kader Kennisveiligheid in te vullen. Voor [het aannemen van nieuwe medewerkers is een factsheet](#) opgesteld die je kunt raadplegen.

¹ Het gaat zowel om medewerkers met een WP- als OBP-functieprofiel.

² Voor een overzicht van de HR-adviseurs en afdelingsmanager per afdeling zie [hier](#).

- b. Indien het gaat om een samenwerkingsovereenkomst, raadpleeg dan de [factsheet 'Houd regie en voorkom afhankelijkheid'](#) en neem eventueel contact op met legal@vu.nl voor het maken van goede contractafspraken. Bij co-auteurschap van manuscripten is alertheid geboden indien de "corresponding author" afkomstig is uit een risicovol land (zie punt 4 [Kader Kennisveiligheid](#)).
2. Wanneer één of meerdere van de vragen van het kader kennisveiligheid met 'ja' zijn beantwoord, of als er twijfels zijn over de beantwoording van de vragen, dan moeten er aanvullende vragen worden beantwoord. De uitgebreide vragenlijst is [hier te vinden](#) en in [Bijlage 2 van het VU Kader Kennisveiligheid](#). Het invullen van deze uitgebreide vragenlijst helpt om het adviserings- en besluitvormingsproces te versnellen.
 3. Stuur de ingevulde aanvullende vragenlijst naar de contactpersonen Kennisveiligheid van de faculteit (Esther van de Hengel en Maaïke Verbree) en informeer het MT van de afdeling via de afdelingsmanager¹.
 4. De contactpersonen Kennisveiligheid besluiten - op grond van de ingevulde vragenlijst - of de samenwerking doorgang kan vinden. Indien er nog onduidelijkheid bestaat, zullen zij de betreffende medewerker vragen om meer informatie. Voor het nemen van een besluit kunnen zij advies vragen aan de Adviesgroep Kennisveiligheid VU. De Adviesgroep Kennisveiligheid VU heeft iedere donderdag online spreekuur.
 5. Uitsluitend de Adviesgroep Kennisveiligheid kan, indien nodig, contact opnemen met het [Landelijk Loket Kennisveiligheid](#) voor aanvullend advies.
 6. De contactpersonen Kennisveiligheid besluiten op basis van de ingevulde aanvullende vragenlijst en, indien nodig, op basis van het advies van de Adviesgroep Kennisveiligheid VU of de samenwerking doorgang kan vinden. In sommige gevallen zal het nodig zijn één of meerdere gesprekken te hebben. De contactpersonen kunnen beargumenteerd afwijken van het advies door de Adviesgroep Kennisveiligheid of het Landelijk Loket Kennisveiligheid. Eventueel wordt de besluitvorming met het Faculteitsbestuur besproken.
 7. Indien de internationale samenwerking doorgang kan vinden, denk dan aan de volgende vervolgstappen:
 - a. Bij het aanstellen van een **nieuwe medewerker**, moet de HR-adviseur worden betrokken;
 - b. Bij het opstellen van een **contract**, wordt contact opgenomen met Legal@vu.nl;
 - c. Bij het ontvangen van **buitenlandse delegaties/bezoek**, worden de adviezen uit het [factsheet](#) gevolgd;
 - d. Bij het maken van een **internationale reis**, zijn de volgende [aandachtspunten](#) van belang.

Als je momenteel een internationale samenwerking hebt en twijfelt of deze is toegestaan, neem dan direct contact op met het MT van de afdeling¹ en de directeur Bedrijfsvoering.

Als je zelf al contact hebt opgenomen met de Adviesgroep Kennisveiligheid, stel dan ook de contactpersonen Kennisveiligheid van de faculteit en het MT van de afdeling op de hoogte van de casus.

Kader kennisveiligheid

Voor het aangaan van nieuwe internationale samenwerkingen, zoals het aanstellen van een nieuwe medewerker, samenwerking met een instelling of contracten met een opdrachtgever

of financier op gebied van onderzoek, onderwijs of bedrijfsvoering zijn de onderstaande 6 vragen leidend:

Voor het doorlopen van de 6 vragen kun je ook het [stroomschema Kennisveiligheid](#) raadplegen. Hieronder staat een samenvatting van het VU Kader Kennisveiligheid met een uitgebreidere toelichting op het stroomschema:

Wettelijk kader: Is het juridisch toegestaan?

1. Staat het bedrijf, de organisatie of het land met wie u wilt gaan samen werken op de EU of VN -sanctie lijst?

Samenwerken met personen, bedrijven, organisaties of landen die voorkomen op de EU- en VN-sanctielijst is strafbaar en dus niet toegestaan.

- Eventuele partnerschappen met Iran en Noord-Korea moeten altijd worden gecontroleerd via de [EU sanctionlist](#). Informatie over de landen is ook te vinden op de volgende website van de overheid: [Landen en regio's](#) (rvo.nl).
- Zie [hier](#) voor instructie hoe je de sanctielijst-check kunt uitvoeren.
- Wat China betreft bestaan er geen formele beperkingen op de samenwerking met wetenschappers, maar kan dit wel gelden voor bepaalde instituten en personen die aan deze instituten (recent <4 jaar) verbonden zijn geweest (zie ook vraag 3).
- Voor Rusland/Belarus(Wit-Rusland) gelden [bijzondere bepalingen](#).
- Voor het aannemen van [nieuwe medewerkers is een factsheet](#) opgesteld met aandachtspunten. Dit geldt voor alle medewerkers, dus zowel met een OBP- als een WP-functieprofiel, gastaanstellingen en tijdelijke aanstellingen (promovendi en postdocs). Betrek hierbij de HR-adviseur. Zij kunnen indien gewenst ook ondersteuning bieden.

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

- Het gaat om (kennis van) producten, programmatuur of technologie (zie [bijlage 1 van de Dual-use verordening](#)) die zowel een civiele als militaire bestemming kunnen hebben.
- Afwegingen daarbij zijn 1) de mate van fundamenteel wetenschappelijk onderzoek gebaseerd op de Technology Readiness Level (TRL) en 2) de openlijke beschikbaarheid van de (kennis over) de producten, programmatuur of technologie vóór de start van het onderzoek.
- Voor dual-use van onderzoek in de levenswetenschappen (bijv. risicovolle ziekteverwekkers), kun je de specifieke [factsheet over biosecurity](#) raadplegen voor meer informatie.
- Ga naar pagina 7 van het [Kader Kennisveiligheid VU](#) voor meer informatie.

Risicobeheersing: Welke risico's zijn er?

3. Is de partner verbonden (geweest) aan een militaire organisatie buiten de EU?

Samenwerkingen met militaire organisaties en daaraan gelieerde instellingen van landen buiten de EU is zeer ongewenst. Screen CV's van personen op recente (<4 jaar) (indirecte) affiliaties.

Voor China geldt dat onderzoeksinstituten die sterke banden hebben met het Chinese leger moeten worden vermeden (in het bijzonder de zogenaamde 'Seven Sons'). Voor deze instituten is de 'ASPI-lijt' te raadplegen ([ASPI unitracker](#)). 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 middelmatig risico kan lopen, maar een specifiek laboratorium binnen dit instituut een (heel) hoog risico kan vormen. Voor de risiconiveaus gelden de volgende uitgangspunten:

- 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 overzicht van de sleuteltechnologieën is [hier te vinden](#).
- Als het gaat om digitale producten, raadpleeg dan ook de [factsheet 'Grappierhauscriteria voor aanbestedingen digitale producten'](#).
- De samenwerking op sensitief onderzoek is ongewenst met risicovolle landen. Het risico kan worden bepaald door een combinatie van de volgende informatiebronnen:
 - Landen die laag (<0.4) scoren op de [Academic Freedom Index](#)
 - Landen met een verhoogd risicoprofiel volgens de [EU-sanctielijst](#) en [dreigingsbeeld](#) van de AIVD

5. Is er 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. Controleer de landenscore op de [Academic Freedom Index](#), bij 0.4 of lager moet dit worden besproken met de directeur Bedrijfsvoering.

6. Is er spraken van eenzijdige externe financiering bij de samenwerking of bij inkomende medewerkers?

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

Het is wel mogelijk om bursalen door de VU te selecteren op een onderwerp dat door de VU is aangedragen en waarbij een promotie op de VU plaatsvindt.

Voor een uitgebreide toelichting over de bovenstaande vragen ga naar pagina 7 en 8 [Kader Kennisveiligheid VU](#).

Additionele informatie

Contacten

- Faculteitsbestuur:
 - Esther van den Hengel: e.i.v.vanden.hengel@vu.nl

- Maaïke Verbree: m.verbree@vu.nl.
- Adviesgroep kennisveiligheid van de VU: kennisveiligheid@vu.nl
- Het MT van de afdelingen³
- HR adviseur van de afdeling²
- Legal services VU: legal@vu.nl.

Pagina's

- [Kennisveiligheid voor VU medewerkers](#)
- [Kader Kennisveiligheid VU](#)
- [Landelijk Loket Kennisveiligheid](#)
- [Nationale leidraad kennisveiligheid](#)
- Het overzicht van de sleuteltechnologieën is [hier](#) te vinden.
- Het [stroomschema](#) met de 6 basisvragen voor de afweging kennisveiligheid
- De uitgebreide vragenlijst is [hier te vinden](#)

³ Voor een overzicht van de afdelingsmanagers en HR-adviseurs per afdeling zie [hier](#).