



The Rights forum

[REDACTED]
Postbus 20565
1001 NN AMSTERDAM

Datum

11-06-2024

Onderwerp

Aanvullend Wob-Besluit Israëlische organisaties

PER E-MAIL:

[REDACTED]

Ons kenmerk

[REDACTED]

Uw kenmerk

[REDACTED]

Pagina

1/7

Bijlagen

1

Afdeling

College van Bestuur

Bezoekadres

Burgerneester Oudlaan 50
Erasmus Building
[REDACTED]

Postadres

Postbus 1738
3000 DR Rotterdam

T [REDACTED]

E woo@eur.nl

W www.eur.nl

Geachte heer [REDACTED]

Inleiding

Naar aanleiding van de mondelinge uitspraak van 14 december 2023 ter zake het beroep met zaaknummer ARN 23 / 2458 WOO 392¹ is het besluit van 6 april 2023 ([REDACTED]) door de rechtbank vernietigd. Daarop is door ons college van bestuur op 12 maart 2024 een nieuw besluit genomen op uw oorspronkelijke WOO aanvraag ter zake de onderdelen 3 en 4.

Naar aanleiding daarvan heeft u een gesprek gehad met een afvaardiging namens de gezamenlijke Colleges van bestuur. U heeft daarbij aangegeven dat in het nieuwe besluit een te beperkte scope is toegepast.

In vervolg op genoemde gesprek heeft u op 30 april 2024 een (pro forma) beroep ingesteld bij de rechtbank Arnhem (ARN 24 / 2609).

Precisering

In het met de vertegenwoordiging namens de gezamenlijke universiteiten gevoerde gesprek heeft u de aanvraag nader gepreciseerd (en schriftelijk bevestigd):

Met betrekking tot verzoek 3: het WOO verzoek betreft tevens e-mail en brief wisselingen die binnekomen bij het bestuur van faculteiten (inclusief archief met betrekking tot de genoemde periode). Er hoeft dus niet verder in de organisatie te worden gezocht, dus niet op departementaal of individueel niveau. Maar alleen op het niveau van het centrale universiteitsbestuur is een te beperkte opvatting.

¹ Afschrift d.d. 20 december 2023

Met betrekking tot verzoek 4: dit gedeelte van het WOO verzoek betreft niet alleen samenwerkingen met organisaties genoemd onder punt 3 van het verzoek maar vooral de bedrijven, instellingen en universiteiten genoemd onder punten 1 en 2.

Maw: in hoeverre worden er bij het aangaan van contracten, samenwerkingsverbanden enz. onderzocht of de resultaten van de samenwerking ook kunnen worden ingezet op een andere wijze dan waarvoor het onderzoek is bedoeld (dual use) of in hoeverre dit bedrijven, universiteiten of instellingen betreft die in een ander opzicht een rol spelen bij mogelijke mensenrechtenschendingen in Israël en Palestina? Bijv. niet alleen dat wordt samengewerkt aan een product dat direct kan worden ingezet om rechten te schenden (dual use), maar ook als wordt samengewerkt aan een ander product, terwijl dat bedrijf/universiteit/instelling daarnaast ook op enige wijze bijdraagt aan bijv. de bezetting van de Westelijke Jordaanoever. Het gaat daarbij zowel om beleid als de toepassing van beleid in concrete gevallen.

Universiteiten openbaren hun beleid met betrekking tot dual use (dat weliswaar niet uitsluitend, maar ook van toepassing is op Israelische samenwerkingen).

Gezien het voorgaande neem ons College van bestuur hierbij een aanvullend besluit.

Publieke informatie

Artikel 4 lid 1 WOO bepaalt dat ieder een verzoek om publieke informatie tot een bestuursorgaan kan richten. Het begrip publieke informatie wordt in artikel 2.1 gedefinieerd als 'informatie neergelegd in documenten die berusten bij een orgaan, persoon of college als bedoeld in artikel 2.2 eerste lid WOO. Een document wordt gedefinieerd als een door een orgaan, persoon of college opgemaakt of ontvangen schriftelijk stuk of andere geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college.

Digitale communicatie

U heeft uw oorspronkelijke aanvraag per e-mail ingediend, bovendien spreekt u in uw e-mail van 4 februari 2022 de voorkeur uit voor verdere digitale communicatie. Dit besluit wordt u hierbij dan ook via uw e-mailadres [REDACTED] toegezonden.

Scope aanvraag

De oorspronkelijke aanvraag luidt:

3. *Alle documenten aangaande formele samenwerking, samenwerkingsprojecten en/of correspondentie met...*
 - a. *de volgende Nederlandse organisaties en hun vertegenwoordigers (in hun capaciteit als vertegenwoordigers):*
 - i. *Centrum voor Informatie en Documentatie Israel (CIDI),*
 - ii. *Christenen voor Israel,*
 - iii. *Centraal Joods Overleg (CJO),*
 - iv. *Dutch Support for Israel,*
 - v. *Federatief Joods Nederland,*
 - vi. *Likoed Nederland,*
 - vii. *StandWithUs Nederland,*
 - viii. *Nationaal Coördinator Antisemitismebestrijding (NCAB, valt onder het ministerie van Justitie en Veiligheid) en*
 - ix. *Stichting Nederlands Industrie voor Defensie en Veiligheid (NIDV) (inclusief NEDS NIDV Exhibition Defense & Security),*
 - b. *en de volgende buitenlandse, Europese en/of internationale organisaties en hun vertegenwoordigers (in hun capaciteit als vertegenwoordigers):*
 - i. *Anti-Defamation League,*
 - ii. *Birtheright Israel,*
 - iii. *Birtheright Israel Foundation,*
 - iv. *Bundesverband RIAS e.V.,*
 - v. *B'nai B'rith International,*
 - vi. *B'nai B'rith Europe,*
 - vii. *EU Coordinator on combating antisemitism and fostering Jewish life,*
 - viii. *International Holocaust Remembrance Alliance (IHRA),*
 - ix. *JNF Charitable Trust (JNF-UK),*
 - x. *Keren Kayemet LeYisrael (JNF-KKL),*
 - xi. *NGO Monitor en*
 - xii. *Simon Wiesenthal Center.*
4. *Alle interne adviezen, mailwisselingen, richtlijnen en andere beleidsstukken waarin is neergelegd of wordt besproken hoe bij (verschillende vormen van) samenwerking met Israëlische universiteiten, bedrijven of organisaties moet worden onderzocht of dergelijke samenwerking op welkelei wijze dan ook zou kunnen bijdragen aan mensenrechtenschendingen in Israël en*

diens stelselmatige onderdrukking, discriminatie, ontegening, en uitsluiting van Palestijnen.

In al het bovenstaande wordt met 'Erasmus University Rotterdam' bedoeld Erasmus University Rotterdam en alle organen die daaronder vallen, waaronder haar commissies, faculteiten, afdelingen, centra en fondsen.

In al het bovenstaande wordt met 'Israëlische universiteiten' bedoeld de volgende instituties, en alle organen die daaronder vallen, waaronder hun bestuursorganen, commissies, faculteiten, afdelingen, centra, en fondsen, etc.:

- Technion - Israel Institute of Technology (IIT),
- Hebrew University of Jerusalem (HUJI),
- Weizmann Institute of Science (WIS),
- Bar-Ilan University (BIU),
- Tel Aviv University (TAU),
- University of Haifa (HU),
- Ben-Gurion University of the Negev (BGU),
- Open University of Israel (OPENU),
- Ariel University (AU) en
- Reichmann University (voorheen 'Herzliya Interdisciplinary Center').

Dit verzoek om informatie is beperkt tot documenten geproduceerd, ontvangen, of behandeld tussen 01-01-2012 en de datum van dit Wob-verzoek.

Uit het proces verbaal van de hoorzitting van 14 december 2023 valt op te maken dat de scope van uw aanvraag zich feitelijk beperkt en de aanvraag nader wordt gepreciseerd tot, zoals uw gemachtigden en de rechter dat formuleerden:

Eiseres: "In het verzoek gaat het om formele correspondentie"

Rechter: "Het gaat niet om contacten tussen individuele personen, maar om officiële contacten tussen deze organisaties en de universiteit"

In een interview in nieuwblad Trouw wordt het voorgaande nogmaals bevestigd:

Verslaggever: "Een deel van uw verzoek is ingewilligd, maar de universiteiten willen geen informatie geven over banden met organisaties die u aanmerkt als pro-israelisch. Waarom ligt uw verzoek zo gevoelig?"

[REDACTED]: "Het gaat ons enkel om de institutionele banden tussen universiteiten en andere organisaties. Net zoals je ook kritisch kunt zijn over academische samenwerking met China. Maar al gauw werd er gedaan alsof we op zoek zijn naar

gegevens van Joodse individuen. De manier waarop het in de publiciteit is gekomen, was uiteindelijk schadelijker dan het WOO-verzoek zelf."

Gezien de aanvullend nader afgestemde precisering wordt de scope evenwel uitgebreid tot:

Met betrekking tot verzoek 3: het WOO verzoek betreft tevens e-mail en brief wisselingen die binnekomen bij het bestuur van faculteiten (inclusief archief met betrekking tot de genoemde periode). Er hoeft dus niet verder in de organisatie te worden gezocht, dus niet op departementaal of individueel niveau. Maar alleen op het niveau van het centrale universiteitsbestuur is een te beperkte opvatting.

Met betrekking tot verzoek 4: dit gedeelte van het WOO verzoek betreft niet alleen samenwerkingen met organisaties genoemd onder punt 3 van het verzoek maar vooral de bedrijven, instellingen en universiteiten genoemd onder punten 1 en 2.

Maw: in hoeverre worden er bij het aangaan van contracten, samenwerkingsverbanden enz. onderzocht of de resultaten van de samenwerking ook kunnen worden ingezet op een andere wijze dan waarvoor het onderzoek is bedoeld (dual use) of in hoeverre dit bedrijven, universiteiten of instellingen betreft die in een ander opzicht een rol spelen bij mogelijke mensenrechtenschendingen in Israël en Palestina? Bijv. niet alleen dat wordt samengewerkt aan een product dat direct kan worden ingezet om rechten te schenden (dual use), maar ook als wordt samengewerkt aan een ander product, terwijl dat bedrijf/universiteit/instellingdaarnaast ook op enige wijze bijdraagt aan bijv. de bezetting van de Westelijke Jordaanoever. Het gaat daarbij zowel om beleid als de toepassing van beleid in concrete gevallen.

Universiteiten openbaren hun beleid met betrekking tot dual use (dat weliswaar niet uitsluitend, maar ook van toepassing is op Israelische samenwerkingen).

De scope beperkt zich daarmee op hoofdlijnen tot

1. De tussen het college van bestuur, de besturen van de faculteiten, en genoemde organisaties gevoerde correspondentie.
2. Het beleid van onze instelling terzake kennisveiligheid, in het bijzonder "dual use".

Inventarisatie

Op basis van voornoemde scope hebben wij geïnventariseerd of, en zo ja welke, documenten beschikbaar zijn. Daarbij is de onderzochte periode voor de onderdelen 3 en 4 van uw aanvraag begrensd van 1 januari 2012 tot de datum van uw oorspronkelijke aanvraag.

Ten aanzien van het kennisveiligheidsbeleid is het beleid onderzocht ten tijde van het onderhavige aanvullende besluit.

Feitelijk is er op basis van het voorgaande onderzoek gedaan naar documenten ter zake formele contacten met onze instelling (college van bestuur en besturen faculteiten) en genoemde organisaties.

De afdeling bestuurlijke zaken van de algemene bestuursdienst beheert de correspondentie van het college van bestuur. Deze afdeling is benaderd met de vraag of zij documenten onder zich hebben binnen de scope van uw aanvraag.

De contacten van de besturen van de faculteiten verlopen via het bureau van de respectievelijke decanen. Intern heeft iedere faculteit² onderzoek gedaan binnen de brede scope van de oorspronkelijke aanvraag.

Tijdens het zoeken naar documenten zijn de navolgende acties verricht:

- Onderzoek databanken
- Onderzoek archieven
- Onderzoek e-mailbestanden

De faculteiten van de EUR hebben na onderzoek aangegeven niet over relevante documenten te beschikken. Ook bestuurlijke zaken heeft geen relevante documenten gevonden.

Bovendien heeft het archief van onze instelling op basis van de oorspronkelijke brede scope een zoekslag gedaan die niets relevant heeft opgeleverd.

Ten aanzien van het beleid kennisveiligheid van onze instelling is de functionaris kennisveiligheid van de afdeling bestuurlijke zaken benaderd. Beleid terzake is momenteel in voorbereiding. In dat kader kan u het "programmavoorstel implementatie

² Erasmus School of Economics (ESE); Erasmus School of Health Policy & Management (ESHPM); Erasmus School of History, Culture & Communication (ESHCC); Erasmus School of Law (ESL); Erasmus School of Philosophy (ESPhil); Erasmus School of Social & Behavioural Sciences (ESSB); International Institute of Social Studies (ISS); Rotterdam School of management (RSM)

kennisveiligheid EUR* worden verstrekt. Dit document wordt u (geanonimiseerd) verstrekt bij dit besluit.

Contact

Voor vragen/opmerkingen aangaande dit besluit kunt u contact opnemen met [REDACTED] directeur Juridische Zaken via [REDACTED]

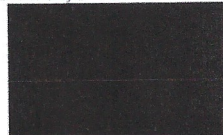
BESLUIT

met inachtneming van het voorgaande, tot:

1. afwijzing van uw aanvraag sub 3 en 4 wegens gebrek aan documenten;
2. openbaarmaking van het "programmavoorstel implementatie kennisveiligheid EUR*" met toezending bij dit besluit.

Hoogachtend,

Het College van Bestuur van de Erasmus Universiteit Rotterdam,



Prof.dr. H. Brinksma
Voorzitter

Niet eens met deze beslissing?

Dan kunt u een bezwaarschrift indienen. Dat kan schriftelijk of per e-mail. Dit moet binnen zes weken na de verzenddatum van dit besluit ter attentie van:

Het College van Bestuur van de Erasmus Universiteit Rotterdam
t.a.v. de Adviescommissie voor Klachten en Bezwaarschriften (AKB)
Postbus 1738 / 3000 DR Rotterdam

Of per e-mail via: akb@eur.nl

In het bezwaarschrift moet in ieder geval staan:

- uw naam, adres en handtekening;
- uw telefoonnummer en e-mailadres;
- de datum waarop u bezwaar maakt;
- een kopie van dit besluit;
- de reden(en) van uw bezwaar

Bent u niet in staat binnen bovengenoemde termijn van zes weken een inhoudelijk bezwaar in te dienen? Dan kunt u binnen diezelfde termijn een inleidend "pro-forma" bezwaarschrift indienen op nader aan te voeren gronden.

Programmavoorstel

Implementatie Kennisveiligheid EUR

Aanleiding

In januari 2022 lanceerde minister Dijkgraaf van OCW de eerste [Nationale Leidraad Kennisveiligheid](#) en het [Landelijke Loket Kennisveiligheid](#)¹. Deze landelijke ontwikkelingen sluiten goed aan bij het [Kader Kennisveiligheid van Universiteiten van Nederland](#) (UNL, 2021). Deze handreikingen bieden belangrijke handvatten en aanbevelingen om kennisveiligheid in relatie tot internationale samenwerkingen beter te borgen binnen de eigen instelling. Dat biedt mogelijkheden om de kansen en (veiligheids)risico's goed en tijdig tegen elkaar af te wegen binnen de eigen instelling. Ook in de [Kamerbrief 'voortgang en vooruitblik aanpak kennisveiligheid hoger onderwijs en wetenschap'](#) wordt immers gesproken over het belang van "versterkte zelfregulering" bij kennisinstellingen.

Via de raden van toezicht zal de minister van OCW erop toezien dat iedere instelling iemand benoemt om de internationale samenwerkingen door te lichten². Ook roept de minister op om in dat kader na de zomer van 2022 een risicoanalyse afgerond te hebben. Inmiddels hebben TU Delft, TU Eindhoven, Universiteit van Utrecht, Universiteit van Leiden en Universiteit van Twente een programmamanager kennisveiligheid aangesteld die verantwoordelijk is voor de risicoanalyse op korte termijn en voor de implementatie van het Kader Kennisveiligheid en de Nationale Leidraad Kennisveiligheid.

Kennisveiligheid in het Hoger Onderwijs

Kennisveiligheid is een betrekkelijk nieuw thema dat nauw samenhangt met academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit. Het is tevens een van de vijf belangrijkste hoofdthema's uit het [Integraal Veiligheidsbeleid 2021-2024 van de EUR](#).

OCW definieert kennisveiligheid in haar Kamerbrief van november 2020 als volgt:

"Bij kennisveiligheid gaat het in de eerste plaats om het voorkomen van ongewenste overdracht van (sensitieve) kennis en technologie, met negatieve gevolgen voor de nationale veiligheid van ons land en aantasting van de Nederlandse innovatiekracht. Daarnaast gaat het ook om heimelijke beïnvloeding van hoger onderwijs en wetenschap door statelijke actoren, die o.a. kan leiden tot vormen van (zelf)censuur met aantasting van de academische vrijheid tot gevolg. Tot slot draait het bij kennisveiligheid om ethische kwesties die kunnen samenhangen met samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd."

Kennisveiligheid raakt meerdere aspecten van veiligheid, denk aan cybersecurity of wetenschappers die heimelijk worden beïnvloed of zelfs bedreigd worden om afstand te nemen van hun academische vrijheid. In het recente Dreigingsbeeld Statelijke Actoren van de Nederlandse inlichtingendiensten komt naar voren dat kennisinstellingen en onderzoeksinstituten "doelwit zijn van spionageactiviteiten door statelijke actoren" (2021). Hoe zien we dit in het licht van onze academische waarden, vrije wetenschapsbeoefening,

¹ Het landelijke loket, dat als contactpunt voor de gehele Rijksoverheid functioneert, is bereikbaar voor alle kennisveiligheid gerelateerde vragen. Op basis van extra informatie en advies kan de kennisinstelling zelf een besluit nemen om internationaal samen te werken.

² Minister Dijkgraaf heeft op 4 april 2022 een brief verstuurd naar alle voorzitters met de oproep te starten met een risicoanalyse. In UNL-verband zal ook gekeken worden hoe andere universiteiten hiermee omgaan.

open science en de talloze internationale (netwerk)samenwerkingen die we als universiteit aangaan met als doel talenten uit te wisselen, kennis te ontwikkelen en te innoveren? Hoe gaan we in die samenwerking om met landen waar bijvoorbeeld de grondrechten niet worden gerespecteerd?

Internationale academische samenwerkingen

Het uitgangspunt is vrij helder: internationale academische samenwerking is van groot belang voor innovatie en kennisuitwisseling en blijft cruciaal voor Nederland als internationaal kennisknooppunt. De zorgen en de risico's nemen echter toe, dus de wijze waarop internationale samenwerking plaatsvindt, dient zo veilig mogelijk te gebeuren: "open waar kan, beschermen waar moet".

Internationale academische samenwerking heeft echter niet alleen betrekking op wetenschappelijk onderzoek en onderwijs. Er zijn ook andere (samenhangende) aspecten die van belang zijn. Denk aan reizen naar het buitenland, het inrichten van IT-systemen en het HR-beleid. Het zijn dus ook de 'ondersteunende' facetten die blootgesteld worden aan de risico's van ongewenste overdracht van informatie en heimelijke beïnvloeding. Om die reden is het van belang om kennisveiligheid breder te borgen in de organisatie.

Nationale actielijnen

Het Kader Kennisveiligheid van UNL formuleert zes actielijnen waar alle universiteiten zich aan hebben gecommitteerd. Deze actielijnen worden ook besproken in de landelijke Werkgroep Kennisveiligheid waar vertegenwoordigers uit het Integrale Veiligheidsnetwerk (IV-Netwerk), waaronder de EUR, aan deelnemen. Het doel is om de actielijnen te vertalen in interne procedures en processen binnen de eigen instelling. Daarbij ligt de focus primair op internationale samenwerkingen met partners uit onvrije landen. Denk aan voorgenomen onderzoeken of internationale samenwerkingsovereenkomsten en consortia. De zes actielijnen zijn:

1. Instellen van een **adviesteam kennisveiligheid** op alle universiteiten, waarin relevante deskundigen over casuïstiek adviseren en expertise opgebouwd en uitgewisseld kan worden.
2. Opstellen van een **landelijke checklist kennisveiligheid**, waarmee risico's rondom kennisveiligheid laagdrempelig te identificeren en te beheersen zijn.
3. **Risico- en incidentenregister** ontwikkelen, waardoor instellingen te allen tijde inzicht hebben in de significante samenwerkingen die ze hebben of aangaan.
4. **Kwaliteits-/auditkader** ontwikkelen, waarmee periodiek wordt geëvalueerd of er relevante veranderingen hebben plaatsgevonden, waarna risico-identificatie, -schatting en -reactie worden heroverwogen.
5. Landelijk ontwikkelen en uitvoeren **trainingen**, voor alle medewerkers toegespitst op risicoprofiel.
6. Landelijke **awareness campagne**, waardoor risico's onder vakgroepen, onderzoekers en diensten verder onder de aandacht worden gebracht.

EUR Status quo

Naar aanleiding van onder andere het Kader Kennisveiligheid heeft het College van Bestuur aan de ABD (AZ & BZ) gevraagd om intern te kijken wat er nodig is om kennisveiligheid naar een hoger plan te tillen. Hieronder de belangrijkste vertrekpunten en bevindingen op basis van verkennende gesprekken en een brainstormsessie met o.a. collega's van ERS, CIO, JZ, AZ en de FG.

- Kennisveiligheid staat niet op zichzelf, maar moet integraal onderdeel zijn van ons doen en laten bij het uitvoeren van onderzoek en onderwijs, inclusief bedrijfsvoering. Daarmee is kennisveiligheid ook een directe lijnverantwoordelijkheid.
- Het is van belang om de verschillende fasen van het proces vanaf de totstandkoming van een onderzoeksidee tot aan onderzoeksvoorstel en honorering helder in kaart te brengen. Dit proces is in de regel decentraal georganiseerd.
- Risico's op het gebied van kennisveiligheid dienen in een zo vroeg mogelijk stadium geïdentificeerd te worden. Het is feitelijk te laat om de voorgenomen internationale samenwerking (onderzoek, consortium etc.) aan kritische toetsing te onderwerpen als bijvoorbeeld de financiering al is afgerond en het onderzoek al van start gaat.
- Een kritische toetsing zou moeten bestaan uit een checklist met vragen die een beeld geven over hoe de internationale samenwerking of voorgenomen onderzoek wordt vormgegeven in relatie tot financiering, (contractuele) borging van academische en democratische waarden, datamanagement en wederkerigheid. Zie bijlage I voor een conceptlijst met vragen over kennisvrijheid en kennisveiligheid.
- Bij een zogeheten 'High Risk Profile' (na een initiële risico identificatie en toetsing) is het van belang dat een multidisciplinair team de risico's zorgvuldig afweegt en adviserend optreedt richting de onderzoeker(s)/faculteiten. Indien nodig is het team ondersteunend aan het College van Bestuur bij bestuurlijke beslissingen over kennisveiligheidskwesties. Een zorgvuldige risicobeoordeling gaat gepaard met het inwinnen van informatie en advies bij het Landelijk loket Kennisveiligheid van de Rijksoverheid.
- Een zorgvuldige risicobeoordeling leidt tot het nemen van mitigerende maatregelen of bewuste beslissingen, waardoor de kans toeneemt dat internationale samenwerkingen op een veiligere manier doorgang vinden.

Voorstel: Adviesteam Kennisveiligheid en Werkgroep Kennisveiligheid

Op basis van de output uit de verkennende gesprekken in samenhang met het Kader Kennisveiligheid UNL en Nationale Leidraad Kennisveiligheid OCW is het voorstel om de komende periode (Q2 t/m Q4) toe te werken naar de uitvoering van de eerste actielijn uit het Kader Kennisveiligheid: het instellen van een centraal adviesteam Kennisveiligheid.

Het Adviesteam Kennisveiligheid bestaat uit relevante EUR-deskundigen die over kennisveiligheidskwesties adviseren op centraal niveau. In relatie tot internationale samenwerkingen en onderzoeken gaat het concreet om de eerder genoemde 'High Risk Profiles'. Het multidisciplinaire Adviesteam adviseert over de risico's en dringt eventueel aan op de te nemen mitigerende maatregelen. Indien de kwestie zeer hoge kennisveiligheidsrisico's kent, wordt het CvB in kennis gesteld. Afhankelijk van het mandaat wordt er op centraal of decentraal niveau een beslissing genomen.

Een centraal Adviesteam Kennisveilig kan pas in werking treden als de nodige processen en procedures op decentraal niveau zijn georganiseerd. Dat betekent dat de 'High Risk Profiles' na een initiële toetsing of vragenlijst op decentraal niveau worden geïdentificeerd en op centraal niveau worden geanalyseerd. Om die reden is het van belang om een al dan niet tijdelijke operationele **Werkgroep Internationale Samenwerking** in het leven te roepen om de processen zodanig decentraal in te richten dat de initiële risico identificatie (en -beoordeling) zo dicht tegen de ontwikkeling van internationale samenwerkingen plaatsvindt.

Programmacoördinator Kennisveiligheid

Het organiseren en coördineren van zowel de operationele Werkgroep als het Adviesteam vraagt om een stevige programmacoördinator die de verschillende proces- en kennisonderdelen aan elkaar weet te verbinden, de schakel is tussen organisatieonderdelen (faculteiten en diensten) en de EUR vertegenwoordigt in diverse landelijke gremia over kennisveiligheid. Een tijdelijke programmamanager/coördinator Kennisveiligheid binnen de EUR zorgt ervoor dat er in korte tijd meer stappen gezet kunnen worden waar de EUR zich bestuurlijk aan heeft gecommitteerd sinds de lancering van het Kader Kennisveiligheid. Dan gaat het niet alleen om internationale samenwerkingen en – onderzoeken, maar ook om bewustwording en heimelijke beïnvloeding van wetenschappers.

De functie van de programmacoördinator Kennisveiligheid zal tijdelijk worden ondergebracht bij Bestuurlijke Zaken (Integrale Veiligheid). Doel hiervan is om het thema aan te jagen binnen de EUR en de eerste stappen te ondernemen die nodig zijn om kennisveiligheid te laten landen binnen de diensten en faculteiten. Op het gebied van zowel beleid als uitvoering en in nauwe samenwerking met betrokkenen. De daadwerkelijke implementatie van diverse processen en procedures rondom kennisveiligheid kan vervolgens – in de lijn – door AZ worden gecoördineerd en geborgd, zodat kennisveiligheid integraal en structureel onderdeel wordt van academische vrijheid, wetenschappelijke integriteit en open science.

Governance

Operationele Werkgroep Kennisveiligheid (tijdelijk)
Leden: <ul style="list-style-type: none">- Coördinator Kennisveiligheid (voorzitter)- ERS vertegenwoordiger- AZ vertegenwoordiger(s)- HR International vertegenwoordiger- EDIS vertegenwoordiger (ISO)- Privacy Officer(s)- JZ vertegenwoordiger(s)- Facultaire vertegenwoordiger(s)
Taken en verantwoordelijkheden
<ul style="list-style-type: none">• Het ontwikkelen en decentraal implementeren van een initiële screening/toetsing/vragenlijst die (hoge) risico's met betrekking tot academische vrijheid en kennisveiligheid aan het licht brengt.• Trainingen ontwikkelen en organiseren voor decentrale medewerkers die in de eerste lijn betrokken zijn bij voorgenomen internationale onderzoeken en/of samenwerkingen, zodat risico's tijdig worden geïdentificeerd en de escalatie naar het centrale Adviesteam plaatsvindt.
Randvoorwaarden
<ul style="list-style-type: none">- Inzet (in uren): 1 uur per week per werkgroep lid- Starten vanaf 1 mei 2022 t/m 1 juni 2023

Stuurgroep en Centraal Adviesteam Kennisveiligheid in wording

Leden: <ul style="list-style-type: none">- Functionaris Gegevensbescherming (FG)- Hoofd Juridische Zaken- Chief Information Security Officer (CISO)

- Hoofd AZ
- Hoofd ERS (ook i.r.t. ethische toetsingscommissie)
- Coördinator Kennisveiligheid
- Adviseur Integrale Veiligheid (voorzitter)

Taken en verantwoordelijkheden

- Internationale samenwerkingen met een hoog risico op kennisveiligheid beoordelen.
- Het CvB adviseren t.a.v. bestuurlijke beslissingen.
- Al doende ontwikkelen van een strategisch (denk)kader dat richting geeft over hoe we omgaan met internationale partners in het licht van onze Erasmian Values.
- Kunnen klankborden met de coördinator Kennisveiligheid over diverse aspecten van kennisveiligheid.

Randvoorwaarden

- Gedurende de periode van de werkgroep: +/- 2 uur per maand
- Wanneer: de stuurgroep blijft parallel aan de werkgroep actief.

Na afronding van de werkgroep en stuurgroep, gaat de stuurgroep over in het Adviesteam Kennisveiligheid dat permanent wordt ingesteld. Inschatting van tijd en werkbelasting is op dit moment moeilijk in te schatten, maar het zwaartepunt ligt met name bij de coördinator kennisveiligheid. Bovendien heeft ieder lid uit het adviesteam een eigen achterban waar eventueel acties uitgezet kunnen worden.

Bijlage I: Conceptlijst vragen voor initiële screening.

Hieronder per onderdeel relevante vragen die aan de voorkant gesteld zouden moeten worden, zodat aspecten van kennisveiligheid geïntegreerd worden in het identificeren en beoordelen van de risico's. Deze vragen zijn afgeleid van het Kader Kennisveiligheid (UNL) en de Nationale Leidraad Kennisveiligheid (OCW).

Samenwerking/ overeenkomst (Internationaal)

- In welke vorm vindt de samenwerking plaats?
- Gaat de overeenkomst uit van wederkerigheid?
 - Denk met name aan de toegankelijkheid en gebruik van onderzoeksdata, maar ook aan vertrouwelijkheid, geheimhoudingsbepalingen en bepalingen over disseminatie en publicatie.
- Bevat de overeenkomst eenduidig geformuleerde ontbindende voorwaarden?
 - Denk aan bepalingen over de manier waarop de samenwerking vorm krijgt; berust op wederzijdse respect met inachtneming van de academische kernwaarden, democratie, internationale grondrechten?
 - Periodieke evaluaties
 - Bepalingen over geschillenbeslechting
 - Hoe zit het met aansprakelijkheid bij vroegtijdige beëindiging van een overeenkomsten?
- Ga na of de samenwerking betrekking heeft op *dual use*-technologie: goederen, software, technologie en informatie die worden gebruikt voor civiele doeleinden, maar die militaire toepassingen kunnen hebben of kunnen bijdragen aan de productie of verspreiding van massavernietigingswapens zoals kernwapens, chemische strijdgassen of biologische wapens.
 - In dat geval is een eindgebruikersverklaring wenselijk.
 - Denk aan Europese Exportregels m.b.t. dual-use goederen en technologie.

Internationale samenwerkingspartners

- Wat is de band tussen een kennisinstelling en diens overheid?
- Is de partner verbonden aan de overheid?
- Wat levert de deelname/bijdrage van de internationale partner(s) op voor de EUR?
- Is de partner verbonden aan het leger of de defensie-industrie?
- Hoe is het gesteld met de academische vrijheid, democratie en respect voor de rechtstaat in het land van herkomst?
- Zijn er sancties op de partner van toepassing?
- Heeft de instelling een aantoonbare reputatie op het vakgebied waar het om gaat?

Datamanagement

- Welke afspraken zijn er gemaakt met betrekking tot de onderzoeksdata- en resultaten?
- Tot welke gebouwen, informatie, onderzoeksresultaten of intern netwerk tot onderzoeksdata en -resultaten krijgen de samenwerkingspartners toegang? Hoe wordt dit tijdens en na afloop van de samenwerking georganiseerd?
- Op welke wijze worden de onderzoeksresultaten gepubliceerd?

Financiering

- Waar komt het geld dat de partner wil investeren vandaan?
- Wat zouden de motieven van de partner kunnen zijn om het onderzoek te financieren?

- Heeft de financier economische of politieke belangen bij een bepaalde uitkomst van het onderzoek?
- Is er informatie te vinden over de opdrachtgever of financier?
- Wordt er gebruik gemaakt van een entiteit die atypisch is voor dit soort onderzoeksfinanciering?
- Wat is het bedrag dat de opdrachtgever/financier beschikbaar stelt en welke financieringsvoorwaarden worden hieraan gesteld?
- De opdrachtgever of financier wil niet dat de resultaten worden gepubliceerd, stelt uitzonderlijk strenge intellectuele eigendomseisen of bedingt geheimhouding t.a.v. eindgebruikers en specificaties.