31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1271 Brief van de minister van Onderwijs, Cultuur en Wetenschap

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 oktober 2026

Op 11 juni jl. heb ik uw Kamer geïnformeerd over de stand van zaken van de screening kennisveiligheid.[1] Een brede screening kennisveiligheid[2] is niet haalbaar gebleken omdat deze niet voldoet aan de criteria van effectiviteit, uitvoerbaarheid en proportionaliteit. Ik voer daarom een haalbaarheidsanalyse uit van een smalle screening kennisveiligheid[3]. Met deze brief informeer ik uw Kamer, mede namens de minister van Economische Zaken en Klimaat (EZK), over de stand van zaken van de haalbaarheidsanalyse.

In het coalitieakkoord is afgesproken dat kennisinstellingen, veiligheidsdiensten en de overheid meer gaan samenwerken om de Nederlandse kennis veilig te houden. Er komt een screeningswet kennisveiligheid die mogelijk maakt dat we, waar nodig, onderzoekers en PhD-studenten die met onze kennis werken kunnen screenen. Dit kabinet zet ambitieus in op het vergroten van publiek-private samenwerking in de onderzoeks- en ontwikkelingsketen. Bijvoorbeeld via initiatieven ontwikkeld vanuit de Taskforce Toekomstige Welvaart en Vestigingsklimaat zoals het Nationaal Groeifonds en het binnenkort aan uw Kamer te zenden Nationaal Programma Defensie Industrie en Innovatie. Daarom wil het kabinet gelijk optrekken met het kennisintensieve bedrijfsleven in het ontwikkelen van deze aanpak en rekening houden met de internationale praktijk.

In de eerder aangekondigde haalbaarheidsanalyse onderzoek ik of het mogelijk zou zijn om te komen tot een smalle screening kennisveiligheid en aan welke voorwaarden moet worden voldaan. Daarnaast onderzoek ik ook alternatieven voor een screening kennisveiligheid. De haalbaarheidsanalyse geeft nog geen definitief uitsluitsel over de uitvoerbaarheid van een smalle screening kennisveiligheid. Dit kan pas in een later stadium worden bepaald, op basis van een concreet nieuw beleidsvoorstel en (concept) wetteksten, waar nieuwe uitvoeringstoetsen en een internetconsultatie over zijn uitgevoerd.

Voor een zorgvuldige afweging betrek ik partijen uit de kennissector bij de haalbaarheidsanalyse. In een klankbordgroep heb ik de voortgang van deze analyse inhoudelijk besproken met experts. Daarnaast bespreek ik de haalbaarheidsanalyse met de bestuurlijke vertegenwoordiging van UNL, NWO, KNAW, UMCNL, VH en de TO2-federatie.

Omdat de benodigde expertise het werkgebied van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) ontstijgt, is betrokkenheid van andere departementen bij de haalbaarheidsanalyse cruciaal. Het ministerie van EZK is bijvoorbeeld verantwoordelijk voor TO2-instellingen; en in het kader van het gelijk speelveld is samenhang met de risicogerichte aanpak van het ministerie

---

[1] Kamerstukken II 2025-2026, 31288, nr. 1260.

[2] Onder een “brede screening kennisveiligheid” verstaat dit kabinet het Wetsvoorstel screening kennisveiligheid dat in 2025 voorlag voor internetconsultatie.

[3] Met een “smalle screening kennisveiligheid” wordt een aangepaste, meer beperkte en gerichtere vorm van screening bedoeld ten opzichte van het Wetsvoorstel screening kennisveiligheid dat in 2025 voorlag voor internetconsultatie.

van EZK van belang voor het tegengaan van ongewenste kennis- en technologieoverdracht (OKTO) via personen in het kennisintensieve bedrijfsleven.

Voortgang haalbaarheidsanalyse smalle screening kennisveiligheid
De haalbaarheidsanalyse richt zich hoofdzakelijk op twee vraagstukken. Ten eerste onderzoek ik een werkbare versmalling van de scope van de screening kennisveiligheid. In de brede screening kennisveiligheid waren alle Nationale Veiligheidsdoelen in de scope opgenomen. Om tot een uitvoerbaar instrument te komen, moeten hier keuzes in gemaakt worden. Dit vertaalt zich in een andere risicoafweging waardoor het aantal sensitieve technologieën dat in de screening kan worden opgenomen minder groot zou moeten zijn. Ik onderzoek wat nodig is om te komen tot een keuze in de scope en technologie

In het kader van bepaling van de scope en het aantal technologieën betrek ik ook de ervaring die ik opdoe met het al bestaande instrument van Verscherpt Toezicht.
Met dat instrument wordt nu al persoonsgericht getoetst om ongewenste kennisoverdracht in het kader van sanctienaleving tegen te gaan. De screening kennisveiligheid beoogt in zekere zin hetzelfde. Het doel hiervan is het tegengaan van OKTO via personen. Bij het Verscherpt Toezicht (VT) zijn de kennisembargo’s uit de VN- en EU-sanctieverordeningen het vertrekpunt. Bij de screening kennisveiligheid is dit de nationale veiligheid in brede zin. Momenteel is het ministerie van OCW samen met het ministerie van Buitenlandse Zaken (BZ) bezig met een actualisatie van de scope van het VT. Deze actualisatie levert waardevolle informatie op die ik meeneem bij de haalbaarheidsanalyse, vanwege de hierboven geschetste parallel tussen de twee instrumenten. In die lijn ben ik voornemens om het VT op korte termijn verder te versterken en verken ik met screeningsautoriteit Justis of zij in 2027 de uitvoering kunnen overnemen, die nu nog bij het ministerie van OCW belegd is. Justis is ook de beoogd uitvoerder van de screening kennisveiligheid, onderdeel van het ministerie van JenV.

De tweede vraag die ik in de haalbaarheidsanalyse onderzoek is op welke wijze ik gelijk kan optrekken met de aanpak van OKTO in het kennisintensieve bedrijfsleven. Hierbij wordt afstemming gezocht met de aanpak Economische Veiligheid waarin de minister van EZK gerichte maatregelen voor het kennisintensieve bedrijfsleven ontwikkelt. Het Dreigingsbeeld Statelijke Actoren (DBSA) 2025 laat zien dat de dreiging van OKTO via personen in beide sectoren bestaat. Dit wordt de *insider threat* genoemd.[4] Hiermee wordt zowel het handelen van kwaadwillenden bedoeld als het onbewust handelen van onderzoekers in hun reguliere uitwisselingen. Het toetsen op en inperken van (de toegang van) personen is een direct aangrijpingspunt om deze risico’s te mitigeren. Ik kijk of de maatregelen die worden getroffen in het bedrijfsleven ook effectief kunnen zijn voor de kennissector.

In deze analyse breng ik ook het belang van een gelijk speelveld tussen de kennisintensieve publieke en private sector in kaart. In mijn afweging neem ik zowel de dreiging als de ambities van dit kabinet mee op het gebied van publiek-private samenwerking in de onderzoeks- en ontwikkelingsketen. Ook kijk ik naar de potentiële ongewenste effecten van een ongelijk nationaal én internationaal speelveld. Daarbij betrek ik effecten op het gebied van een concurrentienadeel van de kennissector ten opzichte van het kennisintensieve bedrijfsleven. En naar potentiële omzeiling van een screening en verschuiving van de dreiging omdat

[4] AIVD, MIVD en NCTV, *Dreigingsbeeld Statelijke Actoren 2025.*

kwaadwillende statelijke actoren hun focus verleggen naar een sector waar geen screeningsmaatregel geldt. Hierbij wil ik ook lessen trekken uit de huidige praktijk van het VT waar eenzelfde soort risico bestaat.

Naast de twee hoofdvragen richt de haalbaarheidsanalyse zich ook op de vraag of het mogelijk is te komen tot een kleinere doelgroepafbakening. Bijvoorbeeld door masterstudenten niet langer mee te nemen in de screening kennisveiligheid. Ik onderzoek onder andere welke bijdrage dit kan leveren aan het versmallen van een screening kennisveiligheid. Tot slot maak ik voor de haalbaarheidsanalyse een inventarisatie van internationaal vergelijkbare initiatieven tot een screening kennisveiligheid.

Verkenning naar alternatieven voor een smalle screening kennisveiligheid
Zoals aangekondigd in mijn brief aan uw Kamer van 11 juni jl. verken ik parallel aan de haalbaarheidsanalyse van een smalle screening ook of er nieuwe en bestaande alternatieven voor een algemene screeningsplicht zijn. Daarbij richt ik mij op instrumenten die aangrijpen op de eerdergenoemde *insider threat*. Ik onderzoek of instrumenten voldoen aan de harde voorwaarde van juridische houdbaarheid en hoe ze uitwerken op het gebied van effectiviteit, uitvoerbaarheid en proportionaliteit.

Ik onderzoek of het mogelijk is andere vormen van screening door de Rijksoverheid in te richten. Daarnaast onderzoek ik of een verplichting voor kennisinstellingen om toegangsbeleid te voeren, zónder screening vooraf door de Rijksoverheid, een alternatief voor een smalle screening kennisveiligheid vormt.

Vervolg
Het effectief beschermen van de Nederlandse kennis staat voor mij voorop. De brede aanpak kennisveiligheid is daarvoor de basis. Ik onderzoek of een smalle screening kennisveiligheid haalbaar zou kunnen zijn, of dit instrument een effectieve bijdrage kan leveren in het tegengaan van de *insider threat* en of samenhang met het bredere kabinetsbeleid kan worden gewaarborgd.

Brede aanpak kennisveiligheid
In de tussentijd werk ik samen met kennisinstellingen aan de doorontwikkeling van de brede aanpak kennisveiligheid. Ik heb een sectorbeeld over 2026 laten opstellen met als belangrijkste doel om inzicht te krijgen in de huidige stand van zaken van de implementatie van de Nationale Leidraad. Dit laat zien dat instellingen duidelijk stappen hebben gemaakt en dat het kennisveiligheidsbeleid binnen instellingen steeds volwassener wordt.[5] UNL en de KNAW en NWO-I hebben een bestuurlijke reactie opgesteld, welke u als bijlage bij deze brief treft. Ik waardeer de gezamenlijke aanpak die we voeren op dit belangrijke thema.

Om deze voortgang te bestendigen is er een flinke financiële impuls beschikbaar gesteld. Zo heeft mijn ambtsvoorganger eerder eenmalig €17,6 miljoen vrijgemaakt en heb ik daarnaast nog €80 miljoen beschikbaar gesteld voor kennisinstellingen. Dat is bijna €100 miljoen voor de kennisinstellingen om digitale en fysieke beschermingsmaatregelen te nemen ten aanzien van kennisontwikkeling en internationale samenwerking.

Verder is deze zomer in nauwe samenwerking met de kennissector een hernieuwde Leidraad Kennisveiligheid gepubliceerd. Dit vormt de basis van het

[5] Kamerstukken II 2025-2026, 31288, nr. 1261.

kennisveiligheidsbeleid in kennisinstellingen en sluit nu weer beter aan bij het huidige volwassenheidsniveau van de sector. Deze nieuwe versie bevat onder andere aanknopingspunten voor kennisveiligheid in personeelsbeleid waarmee kennisinstellingen de *insider threat* zelf tegen kunnen gaan.

Tegelijkertijd is de kennisveiligheidsopgave ook nog niet klaar. Veranderende en voortdurende dreiging vraagt dat we ons blijven inzetten. Daarom ga ik met de sector in gesprek over hoe zij het kennisveiligheidsniveau gaan bereiken dat past bij het risicoprofiel van de betreffende instelling. Ik verwacht van hen concrete voorstellen. Ten eerste hoe kennisinstellingen hun voortgang op kennisveiligheid gaan monitoren en hoe zij dit inzichtelijk maken. Ten tweede hoe kennisinstellingen borgen dat op elk niveau binnen de kennisinstelling (kennis)veiligheid samen met de kansen onderdeel is van de afweging die bij samenwerking wordt gemaakt.

Ook op de doorontwikkeling van het Loket Kennisveiligheid zet ik verder in. Zoals ik aan uw Kamer meldde wil ik het loket versterken met meer brede expertise over sanctie- en exportwetgeving en (sensitieve) technologieën. Daarnaast wil ik in samenwerking met het loket kennisveiligheidsprofielen per instelling opstellen, zodat gerichter beleid kan worden gevoerd en betere ondersteuning kan worden geleverd. Tot slot zet ik mij samen met betrokken instellingen en departementen ook in om internationaal een gelijk speelveld te creëren, bijvoorbeeld door kennisveiligheid meer en beter te verankeren in Europese richtlijnen en verordeningen zoals de European Research Area (ERA) Act, en door de internationale uitwisseling van waardevolle ervaringen en praktijken aan te moedigen. Nederland pakt hierin een
actieve rol op zowel overheidsniveau als door kennisinstellingen zelf. Dit jaar vond in Nederland de eerste grote Europese kennisveiligheidsconferentie voor en door kennisinstellingen plaats, *ENCORS*. Met meer dan 500 bezoekers uit 32 landen een zeer succesvol Nederlands initiatief dat door deelnemers zeer positief is gewaardeerd.

Vervolg haalbaarheidsanalyse smalle screening kennisveiligheid
Het onderzoek naar een smalle screening kennisveiligheid vraagt om zorgvuldigheid. De bevindingen moeten nog worden samengebracht. En met name ten aanzien van de scope van een smalle screening en ten aanzien van het gelijk speelveld met het kennisintensieve bedrijfsleven dient een weging plaats te vinden in het kabinet. In het voorjaar van 2027 verwacht ik uw Kamer te kunnen informeren over de conclusies van deze haalbaarheidsanalyse.

De minister van Onderwijs, Cultuur en Wetenschap,
R.M. Letschert