WIJ WILLEM ALEXANDER,
BIJ DE GRATIE GODS,
KONING DER NEDERLANDEN,
PRINS VAN ORANJE-NASSAU,
ENZ. ENZ. ENZ.

Tijdelijke regels met betrekking tot de advisering van kennisinstellingen over de risico's die gepaard kunnen gaan met internationale samenwerking en andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap (Tijdelijke wet advisering kennisveiligheid)

(KetenID WGK027373)

Voorstel van wet

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is een wettelijke grondslag te bieden voor het adviseren van kennisinstellingen over de risico's die gepaard kunnen gaan met internationale samenwerking en andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap en daarbij de nodige waarborgen op te nemen voor de bescherming van de persoonlijke levenssfeer;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel 1. Begripsbepalingen
In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- *kennisinstelling:* een rechtspersoon die een in de bijlage van de Wet op het hoger onderwijs en wetenschappelijk onderzoek opgenomen instelling of academisch ziekenhuis in stand houdt of is, een rechtspersoon voor hoger onderwijs als bedoeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek dan wel een in de bijlage bij deze wet opgenomen rechtspersoon of organisatie;

- *Onze Minister:* Onze Minister van Onderwijs, Cultuur en Wetenschap.

Artikel 2. Wijziging bijlage
1. Een wijziging van de statutaire naam van een rechtspersoon, genoemd in de bijlage van deze wet, wordt geacht met onmiddellijke ingang te zijn opgenomen in die bijlage.
2. In geval van omzetting, fusie of splitsing van een rechtspersoon als bedoeld in het eerste lid wordt of worden de daaruit voortkomende rechtspersoon of rechtspersonen geacht met onmiddellijke ingang te zijn opgenomen in de bijlage van deze wet.

3. Op de voordracht van Onze Minister kunnen bij algemene maatregel van bestuur rechtspersonen en organisaties aan de bijlage worden toegevoegd, indien de rechtspersoon of organisatie te maken heeft met internationale samenwerking of andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap.

Artikel 3. Openbare lichamen BES
Deze wet is mede van toepassing in de openbare lichamen Bonaire, Sint Eustatius en Saba.

Artikel 4. Taak
1. Onze Minister adviseert kennisinstellingen op verzoek van de kennisinstelling over de risico's die gepaard kunnen gaan met internationale samenwerking en andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap.
2. In verband met de taak, bedoeld in het eerste lid, wordt geen onderzoek gedaan gericht op individuele personen.
3. Bij ministeriële regeling kunnen nadere regels worden gesteld over:
a. de gegevens die de kennisinstelling kan aanleveren bij het verzoek; of
b. de wijze waarop het verzoek wordt ingediend.

Artikel 5. Gegevensverwerking
1. Onze Minister kan ten behoeve van de in artikel 4, eerste lid, bedoelde taak, voor zover dit noodzakelijk is voor de uitoefening van deze taak, gegevens, waaronder persoonsgegevens verwerken:
a. ontvangen op grond van artikel 7, eerste lid;
b. afkomstig uit eerder gegeven adviezen;
c. afkomstig uit publiek toegankelijke bronnen; en
d. ontvangen op grond van artikel 7, tweede lid.
2. Bij het gebruik van de in het eerste lid, onderdeel c, bedoelde bronnen wordt, indien dit onlinebronnen zijn, geen gebruik gemaakt van technische hulpmiddelen die op basis van profilering persoonsgegevens verzamelen, analyseren en combineren.
3. Bij ministeriële regeling worden nadere regels gesteld met betrekking tot de gegevens die op grond van het eerste lid, onderdeel c, gebruikt worden.
4. Bij algemene maatregel van bestuur worden regels gesteld met betrekking tot te nemen technische en organisatorische maatregelen. Dit betreffen in ieder geval regels over autorisatie voor het gebruik van bepaalde systemen, opslag en beveiliging.
5. Persoonsgegevens die op grond van het eerste lid zijn verwerkt, worden in ieder geval uiterlijk vijf jaar na de laatste verwerking vernietigd.
6. Onze Minister is de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens op grond van deze wet.

Artikel 6. Gegevensverstrekkingen door Onze Minister
1. Onze Minister verstrekt aan de kennisinstelling die een adviesverzoek heeft ingediend het advies op het verzoek.
2. Onze Minister verstrekt indien daartoe aanleiding is en voor zover dit noodzakelijk is met het oog op de in artikel 4, eerste lid, bedoelde taak, gegevens, waaronder persoonsgegevens, aan:
a. Onze Minister van Economische Zaken;
b. Onze Minister van Buitenlandse Zaken;
c. Onze Minister van Defensie;
d. Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;
e. indien van toepassing, Onze Minister of Ministers die het mede aangaat.
3. Bij algemene maatregel van bestuur kunnen natuurlijke personen, rechtspersonen of bestuursorganen waaraan Onze Minister gegevens, waaronder persoonsgegevens, kan verstrekken voor zover dit noodzakelijk is met het oog op de in artikel 4, eerste lid, bedoelde taak, worden toegevoegd.

Artikel 7. Gegevensverstrekkingen aan Onze Minister

1. De kennisinstelling die een adviesverzoek indient verstrekt gegevens, waaronder persoonsgegevens, aan Onze Minister voor zover dit noodzakelijk is met het oog op de in artikel 4, eerste lid, bedoelde taak.
2. Voor zover dit noodzakelijk is met het oog op de in artikel 4, eerste lid, bedoelde taak, verstrekken de volgende natuurlijke personen, rechtspersonen of bestuursorganen gegevens, waaronder persoonsgegevens, aan Onze Minister:
a. Onze Minister van Economische Zaken;
b. Onze Minister van Buitenlandse Zaken;
c. Onze Minister van Defensie;
d. Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;
e. Indien van toepassing, Onze Minister of Ministers die het mede aangaat.
3. Bij algemene maatregel van bestuur kunnen natuurlijke personen, rechtspersonen of bestuursorganen die aan Onze Minister gegevens, waaronder persoonsgegevens, kunnen verstrekken voor zover dit noodzakelijk is met het oog op de in artikel 4, eerste lid, bedoelde taak, worden toegevoegd.

Artikel 8. Bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard
1. Gelet op artikel 9, tweede lid, onderdeel g, van de Algemene verordening gegevensbescherming, is het verbod om gegevens waaruit ras of etnische afkomst en politieke, religieuze of levensbeschouwelijke overtuigingen blijken en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid te verwerken niet van toepassing, indien de verwerking geschiedt door Onze Minister, voor zover de verwerking van deze gegevens noodzakelijk is voor de uitoefening van de in artikel 4, eerste lid, bedoelde taak.
2. Gelet op artikel 10 van de Algemene verordening gegevensbescherming kan Onze Minister persoonsgegevens van strafrechtelijke aard verwerken, indien de verwerking noodzakelijk is voor de uitoefening van in artikel 4, eerste lid, bedoelde taak.

Artikel 9. Rechten van betrokkenen
1. Onze Minister kan de verplichtingen en rechten als bedoeld in artikel 23, eerste lid, van de Algemene verordening gegevensbescherming, beperken indien dit noodzakelijk en evenredig is ter waarborging van het in artikel 23, eerste lid, onderdeel a , van die verordening genoemde belang.
2. Indien onze Minister gebruikt maakt van de in het eerste lid bedoelde bevoegdheid, deelt hij dit voorzien van een dragende onderbouwing schriftelijk mee aan de betrokkene wiens rechten worden beperkt.
3. In afwijking van het tweede lid, wordt geen mededeling gedaan aan de betrokkene indien dit afbreuk doet aan het doel van de beperking.

Artikel 10. Evaluatiebepaling
Onze Minister zendt twee jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk.

Artikel 11. Inwerkingtreding
Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld en vervalt op een bij koninklijk besluit te bepalen tijdstip.

Artikel 12. Citeertitel
Deze wet wordt aangehaald als: Tijdelijke wet advisering kennisveiligheid.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Onderwijs, Cultuur en Wetenschap,

Bijlage, behorende bij artikel 1 van de Tijdelijke wet advisering kennisveiligheid

De namen van de privaatrechtelijke rechtspersonen of organisaties in deze bijlage worden weergegeven, zoals zij luiden op DDMMJJJJ.

Rechtspersonen:

- het Centraal Bureau voor de Statistiek, bedoeld in artikel 2 van de Wet op het Centraal bureau voor de statistiek;
- het Centraal Planbureau, bedoeld in artikel 2 van de Wet voorbereiding van de vaststelling van een Centraal Economisch Plan;
- Stichting Deltares te Delft;
- het directoraat-generaal Rijkswaterstaat;
- het Instituut Fysieke Veiligheid, bedoeld in artikel 66 van de Wet veiligheidsregio's;
- het Kennisinstituut voor Mobiliteitsbeleid;
- het KNMI, bedoeld in artikel 2 van de Wet op het Koninklijk Nederlands Meteorologisch Instituut;
- de Koninklijke Nederlandse Akademie van Wetenschappen, bedoeld in artikel 1.16 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek;
- Stichting Koninklijk Nederlands Lucht- en Ruimtevaartcentrum te Amsterdam;
- het Nederlands Forensisch Instituut te 's-Gravenhage;
- Stichting Maritiem Research Instituut Nederland te Wageningen;
- Stichting Naturalis Biodiversity Center te Leiden;
- de Nederlandse organisatie voor wetenschappelijk onderzoek, bedoeld in artikel 2 van de Wet op de Nederlandse organisatie voor wetenschappelijk onderzoek;
- de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek, bedoeld in artikel 3 van de TNO-wet;
- Stichting Nederlandse Wetenschappelijk Onderzoek Instituten te Utrecht;
- het Planbureau voor de Leefomgeving te 's-Gravenhage;
- de Rijksdienst voor het Cultureel Erfgoed;
- het Rijksinstituut voor volksgezondheid en milieu, bedoeld in artikel 2 van de Wet op het RIVM;
- Stichting RKD-Nederlands Instituut voor Kunstgeschiedenis te 's-Gravenhage;
- het Sociaal en Cultureel Planbureau;
- Stichting Wageningen Research te Wageningen;
- Stichting Wetsus, European Centre of Excellence for Sustainable Water Technology te Leeuwarden;
- het Wetenschappelijk Onderzoek- en Datacentrum (WODC)

Memorie van toelichting

Hoofdstuk I. Inleiding

Dit wetsvoorstel regelt een taak van de Minister van Onderwijs, Cultuur en Wetenschap (hierna: de Minister van OCW) inzake de advisering van kennisinstellingen bij het maken van afwegingen over de risico's die gepaard kunnen gaan met internationale samenwerking in het hoger onderwijs en de wetenschap en andere aspecten van kennisveiligheid, en de verwerking van persoonsgegevens bij de uitoefening van deze taak.[1]

Dreigingsbeelden en geopolitieke ontwikkelingen van de afgelopen jaren laten zien dat Nederlandse kennisinstellingen in toenemende mate geconfronteerd worden met handelingen van statelijke actoren gericht op het verkrijgen van hoogwaardige kennis en technologie.[2] Statelijke actoren zetten deze kennis en technologie bijvoorbeeld in voor militaire doeleinden of om de eigen economische en politieke macht te vergroten. Dit kan risico's voor de nationale veiligheid met zich meebrengen, maar zet ook academische kernwaarden zoals de academische vrijheid, internationale samenwerking en open wetenschap onder druk.

In het licht van deze geopolitieke ontwikkelingen werkt de regering sinds enkele jaren samen met de kennissector via verschillende instrumenten aan het versterken en vergroten van de weerbaarheid van het Nederlandse hoger onderwijs en de wetenschap. Het Loket Kennisveiligheid (hierna: het Loket) is een van deze instrumenten. Het Loket is het centrale contactpunt van de hele rijksoverheid, waar kennisinstellingen[3] advies kunnen vragen over risico's rondom internationale samenwerking en andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap. Het Loket is ondergebracht bij de Rijksdienst voor Ondernemend Nederland (hierna: RVO).

Het doel van het Loket is om kennisinstellingen te ondersteunen in het maken van een eigen beoordeling van de kansen en risico's rondom internationale samenwerkingen en andere aspecten van kennisveiligheid. De adviezen zijn juridisch niet-bindend. De verantwoordelijkheid voor het nemen van een besluit over samenwerking op basis van de beschikbare informatie over risico's en hoe die te mitigeren ligt bij het bestuur van de kennisinstelling zelf.[4]

Het Loket voert geen persoonsgericht onderzoek of screening uit bij de uitoefening van haar taak en het Loket doet ook geen uitspraken of een kennisinstelling een persoon wel of niet moet aannemen of toelaten.[5] Tegelijkertijd ontving het ministerie van Onderwijs, Cultuur en Wetenschap twee jaar na oprichting signalen dat het Loket mogelijk persoonsgegevens verwerkt. Dit is als volgt te verklaren: hoewel het Loket geen vragen over personen in behandeling neemt, kan het Loket wel informatie verwerken die voor kennisinstellingen relevant kan zijn om risico's te beoordelen bij het aangaan van samenwerkingen. Die informatie heeft dan betrekking op andere kennisinstellingen waaraan een persoon geaffilieerd is of was, specifieke onderzoeksgebieden waaraan een persoon gaat werken, of de financiering van een bepaald programma. Het is bij het Loket niet bekend rondom welke persoon een kennisinstellingen vragen stelt, en dat is ook niet de bedoeling. Toch kan de combinatie van de gegevens die een kennisinstelling bij het Loket aanlevert wel (indirect) herleidbaar zijn tot een persoon, met name als het gaat om adviesverzoeken in de context van het aannemen of toelaten van personen tot de kennisinstelling. Ook in dat geval is sprake van het verwerken van persoonsgegevens en is daarvoor een wettelijke grondslag nodig.

---

[1] Zie voor de verschillen met het wetsvoorstel screening kennisveiligheid hoofdstuk 2 van deze toelichting.
[2] Dreigingsbeeld Statelijke Actoren (DBSA) 2025.
[3] Zie de artikelsgewijze toelichting bij dit voorstel voor de definitie van kennisinstelling als bedoeld in dit wetsvoorstel.
[4] In de Kamerbrief Uitvoering moties en toezeggingen kennisveiligheid en verscherpt Toezicht (Kamerstukken II 2024/26, 31 288, nr. 1205) wordt een schematische weergave gegeven van de mogelijkheden om in te grijpen wanneer er door wetenschappelijke samenwerking toch een gevaar zou ontstaan voor de nationale veiligheid.
[5] Bij het aannemen of toelaten van een persoon kan bijvoorbeeld worden gedacht aan (gast)onderzoekers, medewerkers of studenten.

Zolang er nog geen wettelijke grondslag bestaat voor het verwerken van persoonsgegevens is de advisering van het Loket over vraagstukken rondom het aannemen of toelaten van personen tot kennisinstellingen ingeperkt. Om dit mogelijk te maken ontvangt het Loket zeer beperkt informatie in deze gevallen, om zo de kans tot een minimum te beperken dat toch persoonsgegevens worden verwerkt. Dit betekent wel dat daarom de adviezen van het Loket algemener van aard zijn en dus minder uitgebreide informatie bevat voor kennisinstellingen om te kunnen gebruiken bij de eigen besluitvorming.

Dit wetsvoorstel is daarom nodig om het Loket zo snel mogelijk weer uitgebreider te kunnen laten adviseren over risico's in de context van het aannemen en toelaten van personen tot een kennisinstelling door het Loket te voorzien van een wettelijke grondslag voor het verwerken van persoonsgegevens voor het geval er onverhoopt gegevens door het Loket worden verwerkt die direct of indirect tot personen te herleiden zijn. Dit wetsvoorstel biedt hiermee nadrukkelijk geen grondslag voor het uitvoeren van een persoonsgericht onderzoek of een persoonsgerichte screening.[6]

Het Loket heeft de status van een project met tijdelijke middelen (tot 2032). Daarom betreft dit een voorstel voor een tijdelijke wet. Na de evaluatie van het Loket (gestart in het najaar van 2025) en de evaluatie van onderhavig wetsvoorstel (twee jaar na inwerkingtreding van dit wetsvoorstel) zal besluitvorming plaatsvinden over het al dan niet structurele karakter van het Loket kennisveiligheid en, in bredere zin, over de taak van Onze Minister omtrent de advisering van kennisinstellingen. Hierbij zal ook worden besloten over de middelen die daarmee gemoeid zijn. Indien na de evaluaties de wens bestaat om de taak van Onze Minister omtrent de advisering van kennisinstellingen structureel te maken, kan onderhavige tijdelijke wet door middel van een wetswijziging alsnog structureel van aard worden gemaakt.

Hoofdstuk 2. Hoofdlijnen van het voorstel

Dit hoofdstuk beschrijft allereerst de achtergrond waartegen dit wetsvoorstel is ontstaan. Daarna wordt een probleembeschrijving gegeven. Vervolgens wordt ingegaan op de taak die met dit voorstel wettelijk wordt vastgelegd.

2.1 Aanleiding en probleembeschrijving

Geopolitieke ontwikkelingen en aanpak kennisveiligheid

Nederlandse kennisinstellingen nemen internationaal een sterke positie in als het gaat om de ontwikkeling en toepassing van hoogwaardige kennis en technologie.[7] De vooraanstaande positie en goede academische reputatie van Nederlandse kennisinstellingen hangen samen met academische kernwaarden zoals de academische vrijheid die in ons land gegarandeerd wordt en de openheid van onze kennisinstellingen naar de wereld.[8] Geopolitieke ontwikkelingen van de afgelopen jaren laten echter zien dat Nederlandse kennisinstellingen vaker geconfronteerd worden met handelingen van statelijke actoren gericht op het verkrijgen van hoogwaardige kennis en technologie, die onze nationale veiligheid kunnen schaden indien de kennis of technologie ongewenste toepassing krijgt. Dit zet de Nederlandse fundamentele academische kernwaarden in toenemende mate onder druk.[9]

Kennisinstellingen en individuele studenten, onderzoekers en medewerkers zijn verder doelwit van statelijke actoren die meningen, publicaties en wetenschappelijk onderzoek proberen te censureren en heimelijk proberen te beïnvloeden. Het kan dan bijvoorbeeld gaan om wetenschappelijk onderzoek naar voor een statelijke actor onwelgevallige onderwerpen, zoals mensenrechtenschendingen en niet alleen over sensitieve kennis of technologie. Ook worden kennisinstellingen geconfronteerd met ethische kwesties rondom internationale samenwerking. Hiervan kan bijvoorbeeld sprake zijn als bepaalde

[6] Overheid.nl | Consultatie Wet screening kennisveiligheid
[7] Nederland scoort al jaren goed op verschillende internationale ranglijsten, zoals de European Innovation Scoreboard en de Global Innovation Index. Binnen de EU doet Nederland mee in de top als het gaat om de ontwikkeling van sleuteltechnologieën, bijvoorbeeld op het gebied van biotechnologie en kwantumtechnologie.
[8] Kamerstukken II 2020/21, 31288, nr. 894.
[9] Kamerstukken II 2022/23, 36200, nr. 213 en Kamerstukken II 2022/23, 30821, nr. 175.

kennis of technologie aan een Nederlandse kennisinstelling wordt verworven en door statelijke actoren wordt ingezet om de eigen bevolking te onderdrukken. Denk aan bepaalde surveillancetechnologie, waarmee statelijke actoren door middel van camera's met gezichtsherkenning de eigen bevolking in de gaten kunnen houden.

In het licht van de geopolitieke ontwikkelingen kondigde de regering op 27 november 2020 in de brief 'Kennisveiligheid hoger onderwijs en wetenschap' een pakket van maatregelen aan die hulp bieden bij het zorgvuldig afwegen van risico's bij internationale samenwerking.[10]

De aanpak kennisveiligheid heeft als doel de weerbaarheid van het Nederlandse hoger onderwijs en de wetenschap vergroten. De rijksoverheid en de kennisinstellingen werken hierbij nauw samen. Kennisinstellingen moeten inzicht hebben in welke belangen zij hebben te beschermen, de risico's hierbij leren herkennen en mitigeren, en maatregelen treffen om ook kansen te kunnen blijven benutten. De rijksoverheid faciliteert kennisinstellingen bij deze inzet op zelfregulering en stelt waar nodig ook wettelijke kaders, zoals met het wetsvoorstel screening kennisveiligheid.[11] Ook voeren de rijksoverheid en de kennisinstellingen doorlopend een dialoog over hoe de aanpak verder kan worden verbeterd, welke dilemma's zich daarbij voordoen en hoe die gezamenlijk kunnen worden opgelost.

Het Loket is in januari 2022 opgericht en is ondergebracht bij de Rijksdienst voor Ondernemend Nederland (RVO), in opdracht van de Minister van Onderwijs, Cultuur en Wetenschap. De Minister van OCW is beleidsverantwoordelijk voor het Loket, en verschillende departementen zijn betrokken bij de advisering en leveren hiervoor inhoudelijke expertise. Het Loket wordt gefinancierd vanuit het Fonds Onderzoek en Wetenschap, dat loopt van 2022 tot 2032.

Het doel van het Loket is om kennisinstellingen op hun verzoek te ondersteunen in het maken van een eigen beoordeling van de kansen en risico's rondom internationale samenwerkingen en andere aspecten van kennisveiligheid. Dit doet het Loket hoofdzakelijk door te adviseren op verzoek van kennisinstellingen. Daarnaast faciliteert de rijksoverheid via het Loket een *learning community*, waarmee het kennisinstellingen actief informeert middels kennissessies, *webinars* en *e-learnings*, en zo onderlinge kennisdeling en bewustwording bevordert.

De adviezen van het Loket zijn juridisch niet-bindend. De verantwoordelijkheid voor de uiteindelijke risicobeoordeling en te nemen maatregelen ligt altijd bij kennisinstellingen zelf.[12] Wanneer (hoge) risico's worden geconstateerd kan het Loket een kennisinstelling dringend adviseren deze risico's te mitigeren. Passende mitigerende maatregelen die het Loket aan instellingen kan meegeven zijn bijvoorbeeld fysieke en digitale beschermingsmaatregelen, voorbereidingen op buitenlandse dienstreizen en bezoek van buitenlandse delegaties, of het opnemen van bepaalde afspraken in een samenwerkingsovereenkomst. In voorkomende gevallen zijn de risico's zo hoog dat het Loket kan adviseren om een samenwerking helemaal niet aan te gaan.

Veel adviesverzoeken van kennisinstellingen gaan over het wel of niet aangaan van intentieverklaringen (MoU's) en/of samenwerkingsovereenkomsten met buitenlandse partnerinstellingen, publiek-private samenwerkingen en deelname met buitenlandse partners aan labs in Nederland of in het buitenland. Daarnaast kan het ook gaan over het aantrekken van buitenlandse onderzoekers en studenten, wederzijdse aanstellingen en promovendi die door het herkomstland worden gefinancierd. Andere voorbeelden van adviesverzoeken zijn vragen over de ontwikkeling van kennisveiligheidsbeleid, de uitleg van sancties, *dual use*[13] en exportcontrole, buitenlandse reizen of lezingen en cybersecurity. Tot slot kan een adviesvraag zien op (mogelijke) heimelijke beïnvloeding

[10] Kamerstukken II 2020/21, 31288, nr. 894.
[11] Overheid.nl | Consultatie Wet screening kennisveiligheid
[12] In de Kamerbrief Uitvoering moties en toezeggingen kennisveiligheid en verscherpt Toezicht (Kamerstukken II 2024/25, 31 288, nr. 1205) wordt een schematische weergave gegeven van de mogelijkheden om in te grijpen wanneer er door wetenschappelijke samenwerking toch een gevaar zou ontstaan voor de nationale veiligheid.
[13] Verordening (EU) 2021/821.

door statelijke actoren of informatie die een instelling nodig heeft voor ethische oordeelsvorming over internationale samenwerkingen.

Met dit wetsvoorstel wordt iets anders geregeld dan met het wetsvoorstel screening kennisveiligheid.[14] Met het wetsvoorstel screening kennisveiligheid is de regering voornemens, daar waar de risico's het grootst zijn en op een beperkt aantal sensitieve technologiegebieden, een persoonsgerichte screening te introduceren. De technologiegebieden en toepassingen die sensitief zijn vanuit het perspectief van nationale veiligheid worden voor de screening kennisveiligheid zo strikt mogelijk afgebakend om het instrument zo risicogericht en proportioneel mogelijk te maken. Het Loket adviseert breder en niet persoonsgericht; namelijk slechts over alle kennis- en technologiegebieden en over alle mogelijke kennisveiligheidsrisico's die kunnen bestaan rondom internationale samenwerkingen. Het bredere kennisveiligheidsbeleid ziet dan ook niet alleen op het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht op een beperkt aantal technologiegebieden, maar ook op heimelijke beïnvloeding en ethische kwesties rondom internationale samenwerking. Het is daarom van belang dat deze beide instrumenten naast elkaar bestaan.

Verwerking van persoonsgegevens door het Loket

Om volledig en precies te kunnen adviseren is het belangrijk dat het Loket gegevens kan verwerken die een volledig beeld geven van de kennisveiligheidsrisico's die kunnen spelen bij het aangaan van internationale samenwerking door kennisinstellingen. Kennisinstellingen hebben behoefte aan ondersteuning vanuit het Loket bij casuïstiek die gaat over risico's voor de nationale veiligheid bij het aannemen of toelaten van personen tot een kennisinstelling. Waar in dit verband wordt gesproken over personen, kan dit gaan over (gast)onderzoekers, medewerkers, studenten of andere personen die verbonden kunnen zijn aan een kennisinstelling.

Naar aanleiding van signalen over de mogelijke verwerking van persoonsgegevens bij adviesverzoeken heeft het Ministerie van OCW twee jaar na oprichting van het Loket een Data Protection Impact Assessment (hierna: DPIA) opgesteld. De DPIA heeft uitgewezen dat het Loket geen persoonsgegevens verwerkt die direct herleidbaar zijn tot een persoon. Wanneer het Loket adviseert over risico's rondom het toelaten, aannemen, of samenwerken met een persoon, is de identiteit van die persoon niet bekend bij het Loket. Het Loket geeft vooraf duidelijk aan geen direct tot personen herleidbare gegevens, zoals een naam, adres of CV van een onderzoeker of student te kunnen ontvangen.[15] Indien dit onverhoopt toch gebeurt, worden deze gegevens direct vernietigd.

Uit de DPIA en gesprekken met de Autoriteit Persoonsgegevens (hierna: AP) blijkt dat het Loket maatregelen heeft getroffen om te zorgen dat bij de advisering ook geen gegevens worden verwerkt die indirect tot personen te herleiden zijn, maar ook dat dit niet volledig uit is te sluiten. Dit werd duidelijk uit de DPIA en uit gesprekken die het Ministerie van OCW met de AP heeft gevoerd. De combinatie van gegevens die bij een adviesverzoek wordt aangeleverd bij het Loket kan in voorkomende gevallen ertoe leiden dat dit indirect herleidbaar is tot een persoon, zeker nu de academische wereld bestaat uit vele internationale netwerken. Denk bijvoorbeeld aan de combinatie van informatie over een potentiële onderzoekspositie, een genoten vooropleiding en affiliaties met kennisinstellingen. Deze gegevens tezamen kunnen herleidbaar zijn tot een persoon. Ook wordt in de DPIA geconcludeerd dat in sommige gevallen bijzondere persoonsgegevens kunnen worden verwerkt. Daarom wordt de grondslag voor de verwerking van bijzondere persoonsgegevens in dit wetsvoorstel opgenomen. In paragraaf 3.1. wordt dit verder toegelicht.

Voor het verwerken van persoonsgegevens, ook als deze slechts indirect herleidbaar zijn tot een persoon, is een wettelijke grondslag nodig.[16] Met dit wetsvoorstel wordt hierin voorzien, maar tot de inwerkingtreding moet zo veel mogelijk worden voorkomen dat het Loket indirect herleidbare (bijzondere) persoonsgegevens verwerkt zonder wettelijke

[14] Overheid.nl | Consultatie Wet screening kennisveiligheid
[15] Zie hiervoor het aanvraagformulier op de website van het Loket: Stel hier uw vraag aan het loket | Loket Kennisveiligheid.
[16] Dit vloeit voort uit artikel 6 van de Algemene verordening gegevensbescherming (AVG).

basis. In de tussentijd zijn daarom tijdelijke maatregelen getroffen die de kans tot een minimum beperken dat toch persoonsgegevens worden verwerkt. Vrijwel alle adviesverzoeken die indirect herleidbare persoonsgegevens bevatten gaan over het aannemen of toelaten van personen tot de instelling die het verzoek heeft ingediend. Om in deze gevallen de ontvangst en verwerking van persoonsgegevens te voorkomen vraagt het Loket aan de aanvrager extra alert te zijn als een adviesverzoek betrekking heeft op de aanstelling of toelating van personen en wordt aangegeven wanneer sprake is van direct en indirect herleidbare persoonsgegevens. Ook geeft het Loket aan welke informatie een adviesverzoek wel en niet mag bevatten. Bij ontvangst van een adviesverzoek controleert het Loket eerst of de aangeleverde gegevens mogelijk (indirect herleidbare) persoonsgegevens bevatten, voordat het adviesverzoek verder in behandeling wordt genomen.

Dit wetsvoorstel is nodig, omdat deze tijdelijke maatregelen ervoor zorgen dat het Loket de adviestaak minder goed kan uitoefenen, omdat het Loket minder specifieke informatie vanuit een kennisinstelling ontvangt. Voor het inschatten van veiligheidsrisico's is de context en de combinatie van factoren immers van belang. Daarom kan het Loket op dit moment minder volledig en precies adviseren over risico's voor de nationale veiligheid bij het aangaan van internationale samenwerking door een kennisinstelling. Kennisinstellingen hebben regelmatig behoefte aan ondersteuning vanuit het Loket bij deze casussen. Zij moeten deze afwegingen nu in grote mate zelf maken, met minder informatie vanuit de rijksoverheid over eventuele risico's en dreigingen. Dit kan ervoor zorgen dat risico's voor de nationale veiligheid minder adequaat worden gesignaleerd en draagt daardoor niet bij aan het vergroten van de weerbaarheid van het Nederlandse hoger onderwijs en de wetenschap. Daarnaast kan het gebrek aan informatie leiden tot het onterecht afwijzen van personen, doordat kennisinstellingen zich moeten baseren op minder informatie bij het maken van risicobeoordelingen. Dit kan onterecht negatieve gevolgen hebben voor de personen in kwestie en de kennisinstellingen zelf.

Hoewel kennisinstellingen vragen stellen over risico's rondom de toelating van personen, voert het Loket geen persoonsgericht onderzoek uit. In artikel 4, tweede lid, van onderhavig voorstel staat dit ook expliciet opgenomen. Het Loket adviseert dan ook niet concreet aan instellingen of zij een persoon wel of niet moeten aannemen of toelaten. Het Loket kan wél adviseren over risico's die uitgaan van statelijke actoren, een specifiek onderzoeksgebied of over risico's rond (buitenlandse) kennisinstellingen en -organisaties. Bij het Loket is in een concreet geval dan ook niet bekend over welke specifieke persoon het gaat bij een verzoek om een advies, omdat deze direct herleidbare gegevens niet mogen worden aangeleverd door een kennisinstelling. Het Loket adviseert in dit soort gevallen alleen over affiliaties van een persoon. Dat het Loket geen persoonsgericht onderzoek doet, wordt ook expliciet duidelijk gemaakt richting de vraagsteller in zowel het aanvraagformulier op de website van het Loket, als in de adviezen zelf. Indien een adviesverzoek desondanks persoonsgegevens (die direct te herleiden zijn tot een persoon) bevat die niet noodzakelijk zijn voor de taakuitoefening van het Loket worden deze direct verwijderd en vernietigd.

Echter, niet alleen bij de aanlevering van gegevens bij de adviesverzoeken kunnen persoonsgegevens worden verwerkt. Ook is het mogelijk dat er tijdens het doen van onderzoek in publiek toegankelijke bronnen en het opstellen van een advies persoonsgegevens worden verwerkt door het Loket. Bijvoorbeeld wanneer een beeld moet worden verkregen van het soort wetenschappelijk onderzoek dat vanuit een bepaalde kennisinstelling wordt uitgevoerd. Hiervoor kijkt het Loket naar de inhoud van publicaties. Daarbij is het haast onvermijdelijk dat ook de namen van betrokken onderzoekers, als auteurs van de publicaties, bekend worden. Het onderzoek richt zich nooit op deze personen, maar in strikte zin worden hun persoonsgegevens dan wel verwerkt, omdat deze gegevens worden gezien. Daarbij speelt mee dat de wetenschap in sterke mate georganiseerd is in specialismen: wetenschappelijke expertise is vaak beperkt tot kleine groepen academici. Ook kan het Loket persoonsgegevens verwerken als mogelijke banden tussen kennisinstellingen worden onderzocht. Dan zoekt het Loket bijvoorbeeld op gezamenlijke publicaties. Ook in dit geval richt het onderzoek zich dan niet op de personen zelf, maar alleen om eventuele banden tussen instellingen.

Met dit voorstel wordt aanvullend een grondslag opgenomen om persoonsgegevens van strafrechtelijke aard te verwerken. Bij een onderzoek naar een kennisinstelling kan namelijk ook specifiek informatie worden gevonden dat een medewerker is vervolgd of veroordeeld voor een relevant strafbaar feit zoals spionage of diefstal van bedrijfsgeheimen. Dit zijn persoonsgegevens van strafrechtelijke aard en dit vereist een specifieke wettelijke grondslag. Dit betekent niet dat er door het Loket gericht onderzoek wordt gedaan naar informatie over mogelijke strafbare gedragingen of veroordelingen van een persoon.

2.2. Taak

Advisering

Onderhavig voorstel legt de bestaande taak van het Loket van de Minister van OCW wettelijk vast, omdat het voor een goede uitvoering van deze taak noodzakelijk is om persoonsgegevens te verwerken. In artikel 4, eerste lid, van onderhavig voorstel is daarom de taak opgenomen dat de Minister van OCW op verzoek van kennisinstellingen adviseert over risico's die gepaard kunnen gaan met internationale samenwerking en over andere aspecten van kennisveiligheid in het hoger onderwijs en de wetenschap. Dit betekent dat alleen de kennisinstellingen die vallen onder het toepassingsbereik van dit wetsvoorstel een adviesverzoek bij het Loket kunnen indienen en dat het Loket alleen adviseert over risico's rondom internationale samenwerking en andere aspecten van kennisveiligheid. In paragraaf 2.1. wordt het begrip kennisveiligheid toegelicht.

Daarnaast is in artikel 4, derde lid, opgenomen dat bij ministeriële regeling nadere regels kunnen worden gesteld over de gegevens die een kennisinstelling kan aanleveren bij het verzoek en over de wijze waarop het verzoek kan worden ingediend.

Kennisinstellingen

In de bijlage bij dit voorstel staat opgesomd welke kennisinstellingen advies kunnen vragen aan het Loket. Dit betreft allereerst de bekostigde en niet-bekostigde instellingen als bedoeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (hierna: WHW). Dit zijn de universiteiten, hogescholen en academische ziekenhuizen. Daarnaast zijn dit de instellingen voor toegepast onderzoek (zogenoemde TO2-instellingen), en instituten van KNAW en NWO. Ook de rijkskennisinstellingen (RKI's) vallen onder het bereik van dit wetsvoorstel.[17] Hoewel deze niet allemaal onder verantwoordelijkheid van de Minister van OCW vallen, voeren zij wel ook wetenschappelijk onderzoek uit en gaan zij internationale wetenschappelijke samenwerkingen aan. Dit betekent dat zij ook geconfronteerd worden met vergelijkbare risico's als de andere kennisinstellingen. Ook werken zij veelvuldig samen met instellingen die wél onder verantwoordelijkheid van de Minister van OCW vallen.

Er is gekozen om bij wet in formele zin de kennisinstellingen aan te wijzen die advies kunnen vragen aan het Loket omdat dit (mede) het toepassingsbereik van het wetsvoorstel bepaalt. Deze kennisinstellingen kunnen in de huidige situatie ook al advies vragen aan het Loket. Gezien de snelle geopolitieke en technologische veranderingen kunnen in de toekomst ook andere kennisinstellingen te maken krijgen met kennisveiligheidsrisico's. Om adequaat op deze ontwikkelingen te kunnen inspelen is in artikel 2, derde lid, van onderhavig voorstel opgenomen dat kennisinstellingen op voordracht van de Minister van OCW middels een algemene maatregel van bestuur kunnen worden toegevoegd aan de bijlage indien deze te maken hebben met internationale samenwerking of andere aspecten van kennisveiligheid. in het hoger onderwijs en de wetenschap.

Gegevensverwerkingen

[17] De RKI's vormen een netwerk aan rijkskennisinstellingen en planbureau's en werken aan onderwerpen zoals veiligheid, gezondheid, economie, onderwijs, leefomgeving en biodiversiteit. Voorbeelden van RKI's zijn het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en het Koninklijk Nederlands Meteorologisch Instituut (KNMI) Rijkskennisinstellingen (RKI).

Het Loket kan op twee momenten persoonsgegevens verwerken.[18] Ten eerste bij de ontvangst van het verzoek om een advies van een kennisinstelling. Ten tweede tijdens het proces van het doen van onderzoek en het opstellen van het advies.

In artikel 5, eerste lid, onder a, van dit voorstel is opgenomen dat het Loket persoonsgegevens kan verwerken die zijn ontvangen bij het verzoek om advies van de kennisinstelling als bedoeld in artikel 4. Het Loket heeft reeds meerdere maatregelen getroffen om ervoor te zorgen dat bij het indienen van een verzoek om een advies de kans wordt beperkt dat er persoonsgegevens worden verwerkt. In het indienformulier voor vragen staat expliciet opgenomen welke gegevens het Loket nodig heeft om een advies op te kunnen stellen, en welke gegevens het Loket niet mag ontvangen. Bij de ontvangst en voor het in behandeling nemen controleert het Loket eerst of de ontvangen gegevens noodzakelijk zijn en geen (mogelijke) persoonsgegevens bevatten. Artikel 4, derde lid, van dit voorstel voorziet tevens in de mogelijkheid om bij ministeriële regeling nadere regels te stellen over de gegevens die de kennisinstelling kan aanleveren bij het verzoek en de wijze waarop het verzoek wordt ingediend. Hiermee kunnen maatregelen worden getroffen om het verwerken van persoonsgegevens tot een minimum te beperken.

Het Loket gebruikt bij het doen van onderzoek en bij het opstellen van een advies met name de informatie die de kennisinstelling aanlevert, informatie uit eerder gegeven adviezen, de expertise van de betrokken departementen en informatie uit publiek toegankelijke bronnen. In de artikelen 5 tot en met 7 van onderhavig voorstel zijn de bepalingen over deze gegevensverwerkingen opgenomen.

Artikel 5, eerste lid, expliciteert in welke gevallen persoonsgegevens kunnen worden verwerkt, voor zover dit noodzakelijk is voor de uitoefening van de advisering door het Loket. In artikel 5, eerste lid, onder b, is een grondslag opgenomen om gegevens te verwerken die afkomstig zijn uit eerder gegeven adviezen. Dit maakt mogelijk dat het Loket bij het opstellen van een advies gebruik kan maken van de inhoud van eerder gegeven adviezen door het Loket. Dit is noodzakelijk, omdat adviezen die eerder zijn opgesteld door het Loket veel relevante informatie bevat die het Loket in voorkomende gevallen kan (her)gebruiken. Dit is ook een belangrijk onderdeel van de kennisopbouw en informatiepositie van het Loket. Tevens voorkomt dit dat voor het opstellen van een nieuw advies opnieuw persoonsgegevens zouden worden verwerkt, terwijl dit niet nodig is voor zover de nieuwe casus overeenkomsten heeft met een eerdere casus. Hieronder wordt onder aparte kopjes achtereenvolgens ingegaan op de gegevens die het Loket verwerkt van de betrokken departementen en het gebruik van informatie uit publiek toegankelijke bronnen.

Gegevensverwerkingen door de backoffice van het Loket

Adviesverzoeken door kennisinstellingen komen bij de frontoffice van het Loket binnen, per e-mail, telefoon of via de website van het Loket. Het Loket neemt alleen verzoeken van personen die werkzaam zijn bij Nederlandse kennisinstellingen in behandeling. De frontoffice beoordeelt vervolgens of de vraag complex is of eenvoudig kan worden afgedaan. Eenvoudige vragen worden door de frontoffice zelfstandig afgedaan.

Bij complexe verzoeken stelt de frontoffice van het Loket een conceptadvies op, waarna dit wordt voorgelegd aan de backoffice van het Loket. De backoffice heeft als taak de medewerkers van RVO met specifieke expertise te ondersteunen bij het opstellen van een advies. De backoffice bestaat - naast medewerkers van RVO - uit deskundige ambtenaren van de ministeries die betrokken zijn bij de brede aanpak kennisveiligheid. Dit betreft het Ministerie van OCW, het Ministerie van Economische Zaken voor expertise over samenwerking met de private sector en het belang van technologieën voor Nederland, het Ministerie van Buitenlandse Zaken voor kennis op het gebied van sanctienaleving en exportcontrole, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Defensie (waaronder de inlichtingen- en veiligheidsdiensten) voor informatie over statelijke dreigingen.

[18] RVO (en daarmee het Loket) wordt na inwerkingtreding van dit wetsvoorstel verwerker, namens de verwerkingsverantwoordelijke de Minister van OCW. Hiertoe wordt ook een verwerkersovereenkomst opgesteld.

In artikel 6 worden de gegevensverwerkingen geregeld die noodzakelijk zijn om gegevens te delen met de kennisinstelling die een verzoek om een advies heeft ingediend en met de betreffende leden van de backoffice. In artikel 6, tweede lid, onder e, is ook geregeld dat gegevens kunnen worden gedeeld met ministers die het mede aangaat, omdat het mogelijk is dat in voorkomende gevallen specifieke expertise nodig is van een minister die normaal gesproken niet bij het Loket betrokken is. Vanuit zijn coördinerende rol ten aanzien van nationale veiligheidsvraagstukken kan het Ministerie van Justitie en Veiligheid incidenteel worden geraadpleegd indien hiertoe een noodzaak bestaat. Andere ministeries kunnen ook ad hoc-basis betrokken worden, wanneer de inhoud van de adviesvraag daartoe aanleiding geeft.

Publiek toegankelijke bronnen

Naast de inbreng van de bij het Loket betrokken departementen en eerder gegeven adviezen, maakt het Loket gebruik van publiek toegankelijke bronnen voor het opstellen van adviezen. Deze publiek toegankelijke bronnen worden ook wel open bronnen genoemd. In artikel 5, eerste lid, onder c, van dit voorstel is de grondslag opgenomen om informatie, waaronder persoonsgegevens, uit publiek toegankelijke bronnen te verwerken door het Loket. In paragraaf 2.1. van dit voorstel wordt de noodzaak van het gebruik van publiek toegankelijke bronnen voor de uitoefening van de taak van het Loket toegelicht.

Publiek toegankelijke bronnen zijn in beginsel alle bronnen die bereikbaar zijn vanaf het internet en niet voorzien zijn van een beveiliging, en waarvan de inhoud bedoeld is om openbaar beschikbaar gesteld te worden. Een bron is dus publiek toegankelijk wanneer daartoe toegang kan worden verkregen zonder een beveiliging te doorbreken of omzeilen, en zonder het aanwenden van technische ingrepen, valse signalen of valse sleutels, of het aannemen van een valse hoedanigheid. Indien een bron vereist dat een account moet worden aangemaakt voordat de bron gebruikt kan worden, is er geen sprake van het doorbreken van een beveiliging en betreft dit een publiek toegankelijke bron. Dit geldt ook voor bronnen waar betaling voor nodig is om toegang te krijgen, zoals betaalde databases.[19] Ingevolge artikel 5, derde lid, van onderhavig voorstel worden bij ministeriële regeling nadere regels gesteld met betrekking tot het verwerken van gegevens uit publiek toegankelijke bronnen, met name over de verschillende categorieën bronnen die gebruikt kunnen worden bij de uitoefening van de taken van het Loket.

Het Loket zal slechts gegevens verwerken uit publiek toegankelijke bronnen, en nooit enige vorm van beveiliging doorbreken om toegang te verkrijgen tot bepaalde informatie. Denk hierbij aan informatie over mogelijk (ongewenste) toepassingen van wetenschappelijk onderzoek, (politieke) gevoeligheid van een bepaald onderzoeksthema, eigendomsstructuren van buitenlandse kennisinstellingen, anderstalige websites van kennisinstellingen, militair onderzoek bij een organisatie, gesanctioneerde kennisinstellingen en vermeldingen van betrokkenen op lijsten met risicovolle entiteiten.

Het onderzoek door middel van publiek toegankelijke bronnen dat door het Loket wordt uitgevoerd is nadrukkelijk niet gericht op personen of anderszins bedoeld om gericht informatie over specifieke personen te verzamelen of te verwerken. Wel kan het zo zijn dat informatie uit publiek toegankelijke bronnen (bijzondere) persoonsgegevens bevatten en het voor de uitvoering van de taak als bedoeld in dit wetsvoorstel noodzakelijk is om ook deze gegevens te verwerken. In paragraaf 2.1. wordt dit nader toegelicht. Opmerking verdient hierbij dat de inbreuk op de persoonlijke levenssfeer die kan volgen uit het verwerken van dergelijke persoonsgegevens altijd zo beperkt mogelijk moet worden gehouden, bijvoorbeeld door het inrichten van werkprocessen en een protocol voor het gebruik van publiek toegankelijke bronnen.

In het voorgestelde artikel 5, tweede lid, is een beperking opgenomen voor het gebruik van technische hulpmiddelen, die op basis van profilering persoonsgegevens of gegevens verzamelen, analyseren en combineren. Dit betekent dat er geen gebruik kan worden

[19] Duidelijke wettelijke kaders rondom het gebruik van publiek toegankelijke bronnen ontbreken momenteel nog. Uit openbare stukken zoals het *juridisch kader online onderzoek in publiek toegankelijke bronnen door gemeenten in het kader van de openbare orde* en de memorie van toelichting bij het wetsvoorstel gegevensvergaring openbare orde geven wel aanknopingspunten.

gemaakt van software die ontworpen is om informatie over personen te profileren of waarbij het risico hierop bestaat.

Kwaliteitsborging adviezen

De adviezen worden opgesteld op basis van per onderwerp opgestelde standaardteksten die interdepartementaal in afstemming tot stand komen. Het advies wordt op maat aangevuld met voor de context relevante informatie afkomstig uit beschikbare bronnen en expertise uit de backoffice. De standaardteksten worden jaarlijks geëvalueerd en waar nodig aangepast. De (jaarlijkse) evaluatie of herijking van het afwegingskader leidt ertoe dat het advies zo risicogestuurd mogelijk is en de daarvoor gebruikte factoren en weging daarvan gebaseerd zijn op actuele informatie over andere dreigingen. Dit leidt tot een zo objectief mogelijk advies en het voorkomen van willekeur. Indien zich nieuwe ontwikkelingen voordoen die verband houden met de standaardteksten dan worden die per omgaande besproken in de backoffice om zo nodig te verwerken in de standaardteksten.

Op basis van de aanwezige expertise en actuele informatie lezen de leden van de backoffice mee op de conceptadviezen en corrigeren waar nodig. Voorafgaand aan verzending van de adviezen vindt op drie lagen controle plaats: voor verzending vindt een laatste check plaats op onder andere consistentie met andere adviezen, logische onderbouwing van de risico-inschatting en volledigheid van de geïdentificeerde risico's.

Hoofdstuk 3. Verhouding tot hoger recht

3.1. De Algemene verordening gegevensbescherming (AVG)

De Algemene verordening gegevensbescherming (AVG) is het wettelijk kader omtrent de bescherming van persoonsgegevens in de Europese Unie. Daarnaast geldt in Nederland de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Deze wet geeft uitvoering aan de AVG voor zover dit de regels betreffen die door lidstatelijk recht kunnen worden gespecificeerd of beperkt. De AVG kan buiten toepassing zijn op de verwerking van persoonsgegevens die lidstaten verrichten bij activiteiten in verband met de nationale veiligheid. Echter, deze uitzondering moet zeer beperkt worden opgevat waardoor de verwerking van persoonsgegevens als bedoeld in onderhavig voorstel valt onder het bereik van de AVG. In Nederland geldt de uitzondering namelijk alleen voor de taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten.[20]

In artikel 4, onder 2, AVG wordt bepaald wat het begrip *verwerking* betekent
De omvang en de aard van de verwerking van persoonsgegevens zullen variëren afhankelijk van de omstandigheden van het geval. Daarom moet ingevolge de AVG worden getoetst of de verwerking van de persoonsgegevens krachtens dit wetsvoorstel voldoet aan de beginselen van gegevensverwerking en rechtmatig plaatsvindt.

De beginselen van gegevensverwerking zijn opgenomen in artikel 5 AVG. Hieronder wordt ingegaan op deze beginselen en hoe daar in dit voorstel invulling aan wordt gegeven.

Artikel 5, eerste lid, onderdeel a, AVG vereist dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene *rechtmatig, behoorlijk en transparant* is. De Minister van OCW en de in artikel 5 aangewezen ministers mogen gegevens verwerken op grond van artikel 6, eerste lid, onderdeel c en e, en artikel 6, derde lid, AVG. Als gegevens verwerkt worden, is dit namelijk noodzakelijk om te voldoen aan de wettelijke verplichtingen die met dit wetsvoorstel worden geïntroduceerd. De verwerking is ook noodzakelijk voor de vervulling van een taak van algemeen belang, die aan de Minister van OCW is opgedragen. Dit betreft het adviseren van kennisinstellingen over de risico's die gepaard kunnen gaan met internationale samenwerking in het hoger onderwijs en de wetenschap en andere aspecten van kennisveiligheid.

[20] De taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten zijn geregeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).

Het beginsel van *doelbinding* zoals neergelegd in artikel 5, eerste lid, onderdeel b, AVG vereist dat persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en dat deze gegevens vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt. Persoonsgegevens worden slechts verwerkt voor zover dat nodig is voor de uitvoering van dit wetsvoorstel. In paragraaf 2.1. en 2.2. staat toegelicht voor welke doeleinden persoonsgegevens worden verwerkt en welke waarborgen hierbij gelden.

Verder mogen persoonsgegevens volgens het beginsel van *minimale gegevensverwerking* alleen worden verwerkt indien zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, ingevolge artikel 5, eerste lid, onderdeel c, AVG. De voor de uitvoering van dit wetsvoorstel relevante persoonsgegevens zijn direct gerelateerd aan de adviestaak van het Loket. De verwerking van de hiervoor geschetste persoonsgegevens is noodzakelijk omdat het Loket anders minder volledig en precies kan adviseren over risico's voor de nationale veiligheid (zie hierover verder paragraaf 2.1.). In paragraaf 2.2. staat toegelicht waarom de gegevensverwerking uit publiek toegankelijke bronnen niet verder gaat dan noodzakelijk is. Er wordt geen gebruik gemaakt van (semi) geautomatiseerde besluitvorming of profilering.

Het beginsel van *juistheid* zoals neergelegd in artikel 5, eerste lid, onderdeel d, AVG vereist dat persoonsgegevens juist zijn en zo nodig worden geactualiseerd en dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. In paragraaf 2.1. onder '*Verwerking van persoonsgegevens door het loket'* staat toegelicht hoe hier in dit voorstel vorm aan wordt gegeven.

Het beginsel van *opslagbeperking* zoals neergelegd in artikel 5, eerste lid, onderdeel e, AVG vereist dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking. In dit wetsvoorstel is daarom een bewaartermijn van vijf jaren opgenomen. Het is van belang om afgegeven adviezen enige tijd te kunnen bewaren, omdat dit een belangrijke kennisbron is voor het Loket en eerder afgegeven adviezen als basis kunnen dienen bij het opstellen van nieuwe adviezen.

Tot slot vereist de AVG dat persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit is het beginsel van *integriteit en vertrouwelijkheid* en is neergelegd in artikel 5, eerste lid, onderdeel f, AVG. Dit betekent dat passende technische en organisatorische maatregelen moeten worden getroffen om hieraan te voldoen. Het Loket neemt hiertoe verregaande beveiligingsmaatregelen bij de verwerking en opslag van de adviesverzoeken en adviezen. Deze maatregelen bestaan uit technische maatregelen om de informatie beter te beschermen, in lijn met de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast zijn er afspraken met alle backoffice-leden over hoe omgegaan moet worden met de informatie uit de adviezen. De naleving van deze maatregelen is een verantwoordelijkheid van RVO. Er is geen formeel toezicht op de naleving door het Loket van vergaande beveiligingsmaatregelen. Wel wordt dit onderwerp besproken in de reguliere cyclus van monitoring en verantwoording van RVO en OCW. Bovendien wordt RVO gevraagd om tegelijk met de uitvoeringstoets een protocol gegevensverwerking op te stellen als extra waarborg.

Voorts is een verwerking alleen rechtmatig indien het voldoet aan ten minste een van de voorwaarden die staan genoemd in artikel 6, eerste lid, AVG. In dit voorstel wordt de rechtmatigheid voor de verwerking van de persoonsgegevens voor de taak als opgenomen in artikel 4, gebaseerd op artikel 6, eerste lid, onderdelen c en e, AVG. Namelijk omdat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust en omdat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang die aan de verwerkingsverantwoordelijke is opgedragen.

Zoals in het derde lid van artikel 6 AVG is opgenomen, geldt dat deze verwerking vastgesteld moet worden bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het onderhavige voorstel regelt deze vaststelling. Daarnaast wordt invulling gegeven aan de hierboven opgenomen beginselen

van verwerking van persoonsgegevens. De AVG vereist dat de verwerking noodzakelijk en evenredig is aan het doel dat met de verwerking wordt nagestreefd.

Ten aanzien van de verwerking van bijzondere persoonsgegevens geldt dat artikel 9, eerste lid, AVG de verwerking van deze gegevens verbiedt. Het tweede lid van artikel 9 bevat vervolgens een limitatief aantal uitzonderingen op dit verbod. Onderdeel g van het tweede lid is in dit kader relevant en bepaalt:

"de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene".

De verwerkingsgrondslag voor bijzondere persoonsgegevens is in artikel 7 van dit wetsvoorstel opgenomen. Bijzondere persoonsgegevens die in het kader van de uitoefening van onderhavig voorstel kunnen worden verwerkt zijn ras of etnische afkomst en politieke, religieuze of levensbeschouwelijke overtuigingen en gegevens over seksueel gedrag of seksuele gerichtheid, bijvoorbeeld indien deze factoren uit de combinatie van gegevens die bij een adviesverzoek worden aangeleverd te herleiden zijn, of wanneer deze gegevens worden geraadpleegd tijdens het doen van onderzoek in publiek toegankelijke bronnen. Een voorbeeld waarin bijzondere persoonsgegevens een rol kunnen spelen ziet op de situatie dat de nationaliteit van een persoon bij het Loket bekend is. Nationaliteit is op zichzelf geen bijzonder persoonsgegeven, maar kan in samenhang met andere gegevens een sterke indicatie van etniciteit of ras opleveren en daarmee wel een bijzonder persoonsgegeven zijn. Het vastleggen van een grondslag voor het verwerken van bijzondere persoonsgegevens neemt niet weg dat zoveel als mogelijk voorkomen dient te worden dat deze gegevens worden verwerkt ter uitvoering van dit voorstel. Het Loket stelt hiertoe een protocol gegevensverwerking op.

Tot slot is in dit wetsvoorstel in artikel 8 de grondslag opgenomen om persoonsgegevens van strafrechtelijke aard te kunnen verwerken, indien de verwerking noodzakelijk is voor de uitoefening van zijn taak op grond van deze wet. Hiervan kan sprake zijn indien het Loket bij het doen van onderzoek naar bijvoorbeeld een kennisinstelling in het buitenland informatie wordt gevonden dat een medewerker op een internationale sanctielijst staat of is vervolgd of veroordeeld voor een strafbaar feit zoals spionage of diefstal van bedrijfsgeheimen.

Rechten van betrokkenen

Bij de taakuitoefening van het Loket worden mogelijk persoonsgegevens verwerkt. De AVG biedt verschillende rechten aan personen wiens persoonsgegevens worden verwerkt. Bijvoorbeeld het recht van inzage van artikel 15 AVG, waarin staat opgenomen dat een betrokken persoon het recht heeft om uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens. Echter, in voorkomende gevallen kunnen deze rechten worden ingeperkt, ingevolge artikel 23 van de AVG en artikel 41 van de UAVG.[21]

Vanuit het oogpunt van het beschermen van de nationale veiligheid van belang dat de inhoud van een advies en andere informatie waar het Loket gebruik van heeft gemaakt vertrouwelijk is en blijft. Hieronder valt ook het deel van de informatie die mogelijk persoonsgegevens bevatten. Met dit voorstel wordt daarom geregeld dat bepaalde rechten van personen die mogelijk bij een adviesverzoek betrokken zijn kunnen worden ingeperkt, omdat dit noodzakelijk is ter bescherming van de nationale veiligheid. In artikel 9 van onderhavig voorstel is de mogelijkheid opgenomen om rechten van

[21] Artikel 23, eerste lid, onderdeel a, AVG voorziet in de mogelijkheid om bij Unierechtelijke of lidstaatrechtelijke wetgevingsmaatregel die op de verwerkingsverantwoordelijke of de verwerker van toepassing is bepaalde rechten van betrokkene te beperken, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van een van de aldaar genoemde belangen. In artikel 41 UAVG is ook de mogelijkheid opgenomen om rechten van betrokkenen onder de aldaar genoemde voorwaarden in te perken.

betrokkenen te beperken met de voorwaarde dat bij gebruikmaking van deze bevoegdheid moet worden voorzien in een dragende onderbouwing, die schriftelijk wordt medegedeeld aan de betrokkene wiens rechten worden beperkt. Indien dit echter afbreuk doet aan het doel van de beperking kan de mededeling aan de betrokkene achterwege worden gelaten.

In dit verband verdient nog opmerking dat wanneer sprake is van een adviesverzoek die (mogelijk) indirect herleidbare persoonsgegevens bevat, bij het Loket vaak ook niet bekend om welke betrokken persoon dit gaat. Het is in dit geval voor het Loket dan ook niet mogelijk, of zou onredelijk veel inspanning vergen, om aan deze betrokken persoon informatie te verstrekken over bijvoorbeeld mogelijke persoonsgegevens die zijn verwerkt.[22]

3.2. Bescherming van de persoonlijke levenssfeer (artikel 8 EVRM, artikel 7 en 8 Handvest van de grondrechten van de Europese Unie, artikel 10 Grondwet)

Met dit wetsvoorstel wordt mogelijk gemaakt dat het Loket in de toekomst kennisinstellingen zo goed mogelijk kan blijven ondersteunen bij het weerbaarder maken van het hoger onderwijs en wetenschap, door het Loket in staat te stellen te adviseren over vraagstukken rondom het aannemen of toelaten van personen tot een instelling en hierbij in voorkomende gevallen persoonsgegevens te verwerken. Onderhavig wetsvoorstel behelst hiermee een beperking van het recht op respect voor het privéleven, respectievelijk een beperking van het recht op bescherming van de persoonlijke levenssfeer. Bescherming van de persoonlijke levenssfeer is een grondrecht dat zowel in nationaal als internationaal recht is vastgelegd.

In deze paragraaf wordt nader ingegaan op de verhouding van onderhavig wetsvoorstel tot deze grondrechten, specifiek artikel 10 van de Grondwet, artikel 8 van het Europees Verdrag van de Rechten van de Mens (hierna: EVRM) en artikel 7 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest).

Ingevolge artikel 10, eerste lid, van de Grondwet heeft een ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. Dit betekent dat beperkingen op dit grondrecht slechts zijn toegestaan indien dit, direct of indirect, herleidbaar is naar een wet in formele zin. Artikel 8 EVRM stelt ook de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven moet zijn voorzien bij wet ("*in accordance with the law*"). Hieruit vloeit voort dat die inmenging moet berusten op een naar behoren bekend gemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. Dit wetsvoorstel voorziet in die wettelijke grondslag voor een gerechtvaardigde beperking op het recht op privéleven.

Artikel 10, tweede en derde lid, van de Grondwet geeft opdrachten aan de wetgever om regels te stellen in het kader van het verwerken van persoonsgegevens. De Algemene verordening gegevensbescherming (AVG) is het wettelijk kader omtrent de bescherming van persoonsgegevens in de Europese Unie. Daarnaast geldt in Nederland de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Deze wet geeft uitvoering aan de AVG voor zover dit de regels betreffen die door lidstatelijk recht kunnen worden gespecificeerd of beperkt.

Voorts is in artikel 8, eerste lid, EVRM het recht van een ieder op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie vastgelegd. Het tweede lid regelt dat geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht dan « voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare

[22] Artikel 14, eerste lid AVG bepaalt dat informatie door een verwerkingsverantwoordelijke moet worden verstrekt wanneer persoonsgegevens niet van de betrokken persoon zelf zijn verkregen. Artikel 14, vijfde lid, onder b AVG bepaalt in deze gevallen dat er geen verplichting bestaat voor de verwerkingsverantwoordelijke om deze informatie te verstrekken, indien dit niet mogelijk is of onevenredig veel inspanning zou vergen.

veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.»

De inmenging in het privéleven op grond van dit wetsvoorstel kan door het belang van de nationale veiligheid worden gerechtvaardigd en dient daarom een legitiem doel. Een inperking is noodzakelijk in een democratische samenleving indien er sprake is van een «pressing social need», oftewel een dringende maatschappelijke behoefte. Het vereiste van proportionaliteit, en van relevante en voldoende redenen voor de inperking, vloeit eveneens voort uit de noodzakelijkheidstoets.

Of een inbreuk voorziet in een dringende maatschappelijke behoefte wordt beoordeeld aan de hand van eventuele minder bezwarende alternatieven (er moet een beredeneerde en gebalanceerde afweging met relevante en voldoende redenen aan de inbreuk ten grondslag liggen) en dat de inbreuk op een effectieve wijze bijdraagt aan het vervullen van de maatschappelijke behoefte. In paragraaf 2.1. staat toegelicht waarom de inbreuk die is voorzien met dit voorstel op deze wijze dient te geschieden en hoe dit bijdraagt aan het vervullen van de maatschappelijke behoefte.

Voorts dient het gebruik van publiek toegankelijke bronnen worden bekeken vanuit het recht op bescherming van de persoonlijke levenssfeer zoals neergelegd in artikel 8 EVRM. Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) maakt in jurisprudentie duidelijk dat 'ook publieke informatie binnen de reikwijdte van het recht op een privéleven valt, voor zover de informatie systematisch wordt vergaard en wordt opgeslagen door overheidsinstanties'.[23] Als publiekelijk beschikbare informatie van internet wordt verzameld en wordt gebruikt, dan brengt dat een inmenging in het recht op privacy als bedoeld in artikel 8 EVRM met zich mee. De persoonsgegevens mogen dan slechts worden verwerkt voor een bepaald doel, voor zover dat bij de wet is voorzien en voor zover dat noodzakelijk is voor het verwezenlijken van dat doel.[24] De eisen die het EHRM stelt aan de wettelijke grondslag voor de onderzoeksbevoegdheid hangen af van de ernst van de privacy-inmenging.

De aard en intensiteit van het openbronnenonderzoek bepalen de eisen die worden gesteld aan de wettelijke grondslag van deze onderzoeksbevoegdheid. Hierbij geldt: hoe groter de inbreuk op de persoonlijke levenssfeer, hoe meer (wettelijke) eisen en waarborgen aan de grondslag moeten worden gesteld. De inbreuk op de persoonlijke levenssfeer door het gebruik van publiek toegankelijke bronnen als bedoeld in onderhavig voorstel is gering, omdat dit niet gericht is op specifieke personen en profilering niet is toegestaan. Gegevens uit publiek toegankelijke bronnen kunnen echter wel persoonsgegevens bevatten en daarom ook worden verwerkt, indien het voor de uitvoering van de taak als bedoeld in dit wetsvoorstel noodzakelijk is. Deze inbreuk op de persoonlijke levenssfeer zal om deze reden dan ook gering zijn. De wettelijke grondslag voor het raadplegen van publiek toegankelijke bronnen als opgenomen in dit voorstel is conform de eisen die het EHRM stelt.

Op EU-niveau is in artikel 7 van het Handvest van de grondrechten van de Europese Unie de eerbiediging van het privéleven opgenomen. Daarnaast is in artikel 8, eerste lid, van het Handvest de bescherming van persoonsgegevens als zelfstandig grondrecht opgenomen. Artikel 52 van het Handvest gaat in op de reikwijdte en uitlegging van de door het Handvest gewaarborgde rechten en beginselen. Artikel 52, derde lid, van het Handvest bepaalt dat – voor zover het Handvest rechten bevat die corresponderen met rechten die al zijn gegarandeerd door het EVRM – in die gevallen de inhoud en reikwijdte ervan hetzelfde is als die er door het EVRM aan worden toegekend. Dit betekent dat hetgeen hierboven is benoemd over artikel 8 EVRM, ook geldt ten aanzien van artikel 7 van het Handvest.

---

[23] EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 43 (*Rotaru/Roemenië*); EHRM 6 juni 2006, 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200, par. 72 (*Segerstedt-Wiberg e.a./Zweden*) en EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 44, (*Uzun/Duitsland*), *EHRC* 2010/123, m.nt. De Hert en Van Caeneghem; en *NJB* 2010/1935 en EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, par. 53 (*Ben Faiza/Frankrijk*), *EHRC* 2018/85, m.nt. Hagens.

[24] Ook art. 5:13 Awb verlangt dat toezichthouders slechts gebruik maken van hun bevoegdheden voor zover dat redelijkerwijs nodig is voor de vervulling van hun taak en voor die evenredigheidstoets is de grootte van de privacy-inbreuk van belang.

In artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU) is het recht van bescherming van persoonsgegevens vastgelegd. Op grond van artikel 16 VWEU is de AVG tot stand gekomen. Op de verhouding van dit voorstel tot de AVG is in paragraaf 3.1. reeds ingegaan.

Hoofdstuk 4. Financiële gevolgen

4.1 Apparaatskosten uitvoering

De Minister van OCW voert de wettelijke taak uit die hij met dit wetsvoorstel krijgt met het Loket Kennisveiligheid. Het Loket is opgericht in 2022. Op basis van eerdere resultaten wordt een uitgave verwacht van ca. €1,9 mln per jaar, aflopend naar €1,7 mln. vanaf 2030. Deze kosten worden reeds gedekt door de Minister van OCW met het Fonds Onderzoek en Wetenschap. De financiering loopt tot 2032.

4.2 Regeldruk: kosten instellingen, bedrijven en burgers

Dit wetsvoorstel heeft geen effect op de regeldruk. Dit wetsvoorstel schept geen nieuwe verplichtingen voor kennisinstellingen, bedrijven of burgers. Ook worden bestaande verplichtingen niet gewijzigd. Het wetsvoorstel biedt een grondslag om nadere regels te stellen over de gegevens die de kennisinstelling kan aanleveren bij het verzoek en de wijze waarop het verzoek wordt ingediend. Een dergelijke ministeriële regeling, voor zover deze zal worden ingevoerd, heeft als doel de kans te verkleinen dat kennisinstellingen persoonsgegevens over derden delen met het Loket Kennisveiligheid. Ook deze regeling zal naar verwachting geen nieuwe verplichtingen voor kennisinstellingen scheppen.

Hoofdstuk 5. Gevolgen (met uitzondering van financiële gevolgen) en Caribisch Nederland

5.1 Gevolgen (met uitzondering van financiële gevolgen)

Een advies kan voor een kennisinstelling mede aanleiding zijn om een persoon geen aanstelling te geven, niet toe te laten tot een studie of geen (onderzoeks)samenwerking met de persoon aan te gaan. De kans dat een kennisinstelling mede op basis van een advies tot een dergelijk besluit komt is groter wanneer het Loket de kennisveiligheidsrisicos als zeer groot of groot inschat. De kans dat een kennisinstelling besluit geen aanstelling, toelating of samenwerking aan te gaan is veel kleiner wanneer het Loket de kennisveiligheidsrisico's als beperkt of zeer beperkt inschat. Tegelijkertijd voorkomt nauwkeurige advisering het onterecht niet aannemen en toelaten van personen, doordat kennisinstellingen zich kunnen baseren op specifiekere informatie over kennisveiligheidsrisico's.

5.2 Caribisch Nederland

Kennisinstellingen kunnen advies vragen op grond van deze wet. In Caribisch Nederland is slechts één kennisinstelling gevestigd, te weten Saba University School of Medicine. Dit is een rechtspersoon voor hoger onderwijs als bedoeld in de WHW.

Hoofdstuk 6. Uitvoering

[Deze paragraaf wordt ingevuld nadat de uitvoeringstoets is gedaan]

Hoofdstuk 7. Toezicht

Het Loket Kennisveiligheid is organisatorisch ondergebracht bij RVO. De plaatsvervangend secretaris-generaal (pSG) van het ministerie van Economische Zaken (EZ) is als eigenaar van het agentschap RVO verantwoordelijk voor het toezicht op het beleid van RVO en op de algemene gang van zaken. Dit geldt ook voor het Loket dat hier organisatorisch is ondergebracht.

De pSG van het ministerie van EZ draagt zorg voor het inrichten van het sturingsmodel, de continuïteit van RVO op lange termijn en het toetsen en goedkeuren van de begroting, de tarieven, het jaarplan, de leenaanvragen en de jaarrekening van RVO. Voor de aansturing door de pSG draait RVO mee in de managementcyclus van het ministerie van EZ. RVO stelt in dit kader jaarlijks managementafspraken (tegenwoordig

jaarplannen) op waarin de te bereiken doelen voor het komend jaar worden vastgelegd. De managementafspraken zijn ondertekend door de pSG van het ministerie van EZ en de algemeen directeur van RVO. Monitoring en verantwoording vindt plaats op basis van een voortgangsrapportage en de jaarverantwoording aan de pSG.

Daarnaast houdt de functionaris gegevensbescherming van EZ ook binnen RVO intern toezicht op de toepassing en naleving van de privacywetgeving. RVO heeft met de Autoriteit Persoonsgegevens van doen voor wat betreft het formele toezicht op de naleving van de privacywetgeving. Ook controleert de ADR op verzoek de jaarrekeningen van agentschappen en van andere onderdelen van een ministerie.

Hoofdstuk 8. Advies en consultatie
[Deze paragraaf wordt ingevuld na de internetconsultatie]

Hoofdstuk 9. Inwerkingtreding
Zie de artikelsgewijze toelichting bij artikel 10 en de laatste alinea van hoofdstuk 1 van het algemeen deel van de memorie van toelichting voor de onderbouwing van de inwerkingtreding.

II. Artikelsgewijze toelichting

Artikel 1. Begripsbepalingen

Dit artikel bevat de benodigde begripsbepalingen van het voorstel.

Onder het begrip 'kennisinstelling' valt voor dit wetsvoorstel een aantal categorieën van rechtspersonen:
1. Rechtspersonen die een in de bijlage van de WHW opgenomen instelling of academisch ziekenhuis in stand houden of zijn.
Dit betreffen de zogenoemde bekostigde hoger onderwijsinstellingen en academische ziekenhuizen.
2. De rechtspersonen voor hoger onderwijs (als bedoeld in de WHW).
Dit zijn de zogenoemde niet-bekostigde hoger onderwijsinstellingen. Dit zijn rechtspersonen die geaccrediteerde initiële opleidingen en postinitiële masteropleidingen verzorgen met uitzondering van de Staat.
3. De in bijlage 1 bij deze wet opgenomen rechtspersonen of organisaties.
Voor deze rechtspersonen of organisaties is geen overkoepelende definitie beschikbaar. Deze rechtspersonen worden daarom in de eerste bijlage bij deze wet aangewezen. Voor de Koninklijke Nederlandse Akademie van Wetenschappen, de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek en de Nederlandse organisatie voor wetenschappelijk onderzoek geldt dat ook alle hieronder vallende instituten onder het toepassingsbereik van dit voorstel vallen. In deze bijlage zijn ook de zogenoemde rijksinstellingen aangewezen.

Onder 'Onze Minister' wordt verstaan de Minister van Onderwijs, Cultuur en Wetenschap, die de eerstverantwoordelijke minister is voor de advisering over kennisveiligheid.

Artikel 2. Wijziging bijlage

In het eerste lid is bepaald dat een wijziging van de statutaire naam van een rechtspersoon, opgenomen in de bijlage bij deze wet, wordt geacht met onmiddellijke ingang te zijn opgenomen in die bijlage.

In het tweede lid is bepaald dat hetzelfde geldt bij een omzetting, fusie of splitsing van een rechtspersoon.

Het derde lid bevat een grondslag om bij algemene maatregel van bestuur rechtspersonen en organisaties aan de bijlage toe te voegen. Dit kan alleen, indien het een rechtspersoon of organisatie betreft die te maken heeft met internationale

samenwerking in het hoger onderwijs en de wetenschap. Die samenwerking hoeft nog niet actueel te zijn. Als er indicaties zijn dat de rechtspersoon of organisatie binnenkort te maken krijgt met internationale samenwerking kan deze ook worden toegevoegd.

Artikel 3. Openbare lichamen BES

Dit artikel regelt dat deze wet ook van toepassing is in de openbare lichamen Bonaire, Sint Eustatius en Saba.

Artikel 4. Taak

Dit artikel beschrijft de taak van de Minister van OCW op het terrein van advisering van kennisinstellingen (zie over het begrip 'kennisinstelling' verder de artikelsgewijze toelichting bij artikel 1). De Minister van OCW heeft geen expliciete taak met betrekking tot het adviseren van andere instellingen dan de kennisinstellingen zoals bedoeld in artikel 1 van deze wet en de bijlage behorende bij dit artikel. De taak wordt in praktijk uitgevoerd door het zogenoemde Loket Kennisveiligheid.

Op grond van dit artikel kan de Minister van OCW op verzoek van de kennisinstellingen adviseren over risico's die gepaard kunnen gaan met internationale samenwerkingen in het hoger onderwijs en de wetenschap en andere aspecten rondom het thema kennisveiligheid. Hoewel de Minister van OCW ook ongevraagd kan adviseren over bijvoorbeeld risico's omtrent internationale samenwerkingen, kunnen ten behoeve van deze ongevraagde advisering geen persoonsgegevens worden verwerkt. De adviesverzoeken zijn uiteenlopend en kunnen bijvoorbeeld zien op een inkoop die een kennisinstelling wil doen of een buitenlandse instituut of wetenschapper waarmee een instelling wil samenwerken. De adviezen zijn juridisch niet bindend van aard.

Uit het tweede lid volgt dat de Minister van OCW bij de uitoefening van zijn taak geen onderzoek of screening verricht dat gericht is op individuele personen. Dit betekent dat het onderzoek dat door het Loket Kennisveiligheid wordt uitgevoerd, zich niet richt op individuele personen en niet wordt ingezet om gerichte informatie over specifieke personen te verzamelen of te verwerken. Kennisinstellingen kunnen wel vragen stellen over risico's rondom de toelating van personen, maar het adviesverzoek van de kennisinstelling zal in de regel geen direct herleidbare persoonsgegevens bevatten. Indien het adviesverzoek wel direct herleidbare persoonsgegevens bevat, worden deze door het Loket vernietigd. De medewerkers van het Loket Kennisveiligheid weten dus bij het uitbrengen van een advies niet welk individueel persoon het betreft. Daarnaast is het onderzoek dat wordt verricht naar aanleiding van een adviesverzoek niet op individuele personen gericht. Het onderzoek richt zich bijvoorbeeld op de risico's die uitgaan van statelijke actoren of risico's rondom andere (buitenlandse) kennisinstellingen. Hoewel er tijdens dit onderzoek indirect herleidbare dan wel herleidbare persoonsgegevens kunnen worden verwerkt, is het onderzoek niet als zodanig *gericht* op de personen wiens gegevens worden verwerkt. Zie voor nadere toelichting paragraaf 2.1 van de algemene toelichting.

Het derde lid bevat een grondslag om nadere regels te stellen over het adviesverzoek dat kennisinstellingen indienen bij het Loket Kennisveiligheid.

Artikel 5. Gegevensverwerking

Uit de combinatie van artikel 6, eerste lid, onderdelen c en e, van de Algemene verordening gegevensbescherming en artikel 5, eerste lid, van onderhavig voorstel volgt dat de Minister van OCW persoonsgegevens kan verwerken ter uitvoering van de in artikel 4, eerste lid, opgenomen taak. Artikel 5 bevat nadere voorschriften ten aanzien van deze verwerking.

In het eerste lid staat dat de Minister van OCW 'gegevens, waaronder persoonsgegevens', kan verwerken. Voor deze formulering is gekozen om te benadrukken dat de Minister van OCW verschillende soorten gegevens verwerkt voor de uitvoering van de in artikel 4, eerste lid, opgenomen taak. De nadere voorschriften in dit artikel hebben echter alleen betrekking op de verwerking van persoonsgegevens. Voor de verwerking van andersoortige gegevens is immers geen wettelijke grondslag nodig.

Op grond van het eerste lid kunnen ten eerste persoonsgegevens worden verwerkt die de kennisinstelling heeft verstrekt. Dit betreft de (indirecte) persoonsgegevens die het adviesverzoek gericht aan het Loket Kennisveiligheid kan bevatten (onderdeel a). Voorts kunnen uitsluitend persoonsgegevens worden verwerkt die afkomstig zijn uit eerder gegeven adviezen door het Loket Kennisveiligheid (onderdeel b) en publieke bronnen (onderdeel c) alsmede persoonsgegevens die zijn verstrekt door andere (overheids)organisaties ten behoeve van de in artikel 4, eerste lid, opgenomen taak (onderdeel d). In de praktijk zullen de personen werkzaam voor of ten behoeve van het Loket Kennisveiligheid nadat zij een adviesverzoek binnenkrijgen eerst kijken naar eerder gegeven adviezen en publiek toegankelijke bronnen om tot een advies te komen. Daarnaast worden vertegenwoordigers van de betrokken ministeries verzocht om mee te denken met het adviesverzoek en input te leveren voor zover deze input noodzakelijk is om te komen tot een gedegen advies. Dit betreft veelal specialistische kennis die zich bevindt bij het betrokken ministerie in kwestie. Er wordt geen onderzoek gedaan gericht op personen. Het Loket richt zich op institutionele en wetenschappelijke informatie en affiliaties. Voor persoonsgericht onderzoek werkt de regering aan het eerdergenoemde wetsvoorstel screening kennisveiligheid (zie nader de toelichting op artikel 4, tweede lid, en paragraaf 2.1 van de algemene toelichting).

Het tweede lid bevat een nadere inperking ten aanzien van het gebruik van de in het eerste lid, onderdeel c, opgenomen publiek toegankelijke bronnen, voor zover het daarbij gaat om online bronnen. Deze beperking betekent concreet dat er geen gebruik kan worden gemaakt van software die ontworpen is om te profileren, bijvoorbeeld zogenaamde 'web crawlers'.

Het derde lid bevat een delegatiegrondslag om bij ministeriële regeling meer duiding te geven omtrent gegevens die worden verzameld uit publiek toegankelijke bronnen en gebruikt bij het opstellen van een advies ter uitvoering van de wettelijke taak.

Het vierde lid bevat een delegatiegrondslag om in een algemene maatregel van bestuur nadere regels te stellen met betrekking tot de te nemen technische en organisatorische maatregelen. De te stellen nadere regels zouden gelden voor alle verwerkingen van persoonsgegevens op basis van onderhavig voorstel, met dien verstande dat afhankelijk van het type verwerking en het soort gegevens maatwerk nodig kan zijn.

Uit het vijfde lid volgt dat de bewaartermijn voor persoonsgegevens die zijn verwerkt op grond van onderhavige wet, uiterlijk vijf jaar na de laatste verwerking is. Hoewel de AVG geen specifieke bewaartermijnen voorschrijft, mogen persoonsgegevens niet langer bewaard worden dan noodzakelijk voor het doel waarvoor ze zijn verzameld (artikel 5, lid, onder e). Deze bewaartermijn wordt proportioneel geacht voor het goed kunnen adviseren op adviesverzoeken omtrent de risico's die gepaard kunnen gaan met internationale samenwerkingen in het hoger onderwijs en de wetenschap. Er is een noodzaak tot bewaring van persoonsgegevens, omdat eerdere adviezen worden gebruikt om te komen tot adviezen op vergelijkbare actuele adviesverzoeken. Er geldt dat (vergelijkbare) casuïstiek zich over meerdere jaren kan uitspreiden. Met deze bewaartermijn wordt bovendien aangesloten bij andere wetgeving waaruit blijkt dat die termijn gebruikelijk of in ieder geval niet ongebruikelijk is. Zo bevat de Wet coördinatie terrorismebestrijding en nationale veiligheid ook deze bewaartermijn. In de memorie van toelichting bij die wet is toegelicht dat om ontwikkelingen van recenter aard te kunnen duiden, het noodzakelijk is om over langere tijd terug te kunnen kijken naar

eerdere ontwikkelingen binnen een bepaald fenomeen, zodat er een beter historisch en contextueel beeld bestaat. Een termijn van vijf jaar wordt van groot belang geacht 'voor een complete en gedegen duiding van fenomenen'.[25] Voor de adviezen van het Loket kennisveiligheid geldt eenzelfde redenering. De bewaartermijn van vijf jaar betreft echter wel een uiterste termijn, wat betekent dat persoonsgegevens ook kunnen worden vernietigd voordat een termijn van vijf jaar is verstreken.

Op grond van het zesde lid is de Minister van Onderwijs, Cultuur en Wetenschap de verwerkingsverantwoordelijke als bedoeld in artikel 4, zevende lid, van de AVG.

Artikel 6. Gegevensverstrekking door Onze Minister

Dit artikel beschrijft aan welke personen en organisaties de Minister van OCW gegevens, waaronder persoonsgegevens, kan verstrekken in het kader van onderhavige wet. Het zal hier veelal gaan om het verstrekken van het adviesverzoek dan wel het advies, dat (indirecte) persoonsgegevens kan bevatten.

Er is gekozen voor de formulering 'gegevens, waaronder persoonsgegevens'. Dit is bedoeld om te benadrukken dat de Minister van OCW verschillende soorten gegevens verstrekt aan de genoemde personen en organisaties met het oog op de in artikel 4, eerste lid, bedoelde taak. De nadere voorschriften in dit artikel hebben echter alleen betrekking op de verstrekking van persoonsgegevens. Voor de verstrekking van andersoortige gegevens is immers geen wettelijke grondslag nodig.

Op grond van het eerste lid verstrekt Onze Minister het advies op het verzoek aan de kennisinstelling die dat adviesverzoek heeft ingediend.

Op grond van het tweede lid kan Onze Minister ook aan een aantal Ministers gegevens, waaronder persoonsgegevens, verstrekken. Het gaat hierbij om verstrekking van het adviesverzoek en de onderhavige casus aan het zogenoemde 'backoffice' van het Loket Kennisveiligheid. Vertegenwoordigers van een aantal ministeries hebben een vaste plek in het 'backoffice', omdat er zich relevante specialistische kennis bevindt bij deze ministeries. De ministeries die tijdens het schrijven van dit wetsvoorstel bij het 'backoffice' betrokken zijn worden in dit artikel genoemd. Daarnaast biedt onderdeel e de mogelijkheid om ook zogenaamde 'vakministers' te betrekken indien dit nodig is. Hierbij kan bijvoorbeeld gedacht worden aan de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur en de Minister van Justitie en Veiligheid. Hoewel zij niet vast vertegenwoordigd zijn in het 'backoffice' worden zij wel op incidentele basis betrokken bij een casus. Daarnaast kan gedacht worden aan de Minister van Volksgezondheid, Welzijn en Sport. Hoewel er nog geen vertegenwoordiger van dit ministerie deelneemt in het 'backoffice', is het goed denkbaar dat er zich in de toekomst een casus voordoet waarvoor specialistische kennis nodig is die zich bij dit ministerie bevindt. Onderdeel f biedt de grondslag om een dergelijk geval de vakminister te kunnen betrekken bij het adviesverzoek op het moment dat het verzoek nog actueel is en niet slechts naderhand.

Het derde lid biedt een grondslag om bij algemene maatregel van bestuur partijen toe te voegen waaraan Onze Minister persoonsgegevens kan verstrekken. Als bijvoorbeeld blijkt dat het nodig is dat vertegenwoordigers van ministeries die nog niet genoemd zijn in artikel 6, lid 2, onderdelen a tot en met d, op meer vaste basis te laten aansluiten in de 'backoffice' van het Loket Kennisveiligheid, is het voor de voorzienbaarheid en kenbaarheid goed om hen toe te voegen aan de partijen aan wie Onze Minister persoonsgegevens kan verstrekken in het kader van onderhavige wet. Het zal dan gaan om vertegenwoordigers van ministeries waarvan verwacht wordt dat meermaals een beroep zal worden gedaan op hun expertise. Anders zou immers het tweede lid, onderdeel e reeds een uitkomst bieden.

[25] Zie Kamerstukken II 2021/22, 35958, nr. 3, p. 22.

Artikel 7. Gegevensverstrekking aan Onze Minister

Dit artikel beschrijft welke personen en organisaties aan de Minister van OCW gegevens, waaronder persoonsgegevens, kunnen verstrekken in het kader van onderhavige wet. Het zal hier veelal gaan om het verstrekken van het adviesverzoek dan wel input op het adviesverzoek.

Er is gekozen voor de formulering 'gegevens, waaronder persoonsgegevens'. Dit is bedoeld om te benadrukken dat de Minister van OCW verschillende soorten gegevens ontvangt van de genoemde personen en organisaties met het oog op de in artikel 4, eerste lid, bedoelde taak. De nadere voorschriften in dit artikel hebben echter alleen betrekking op de verstrekking van persoonsgegevens aan de Minister van OCW. Voor de verstrekking van andersoortige gegevens is immers geen wettelijke grondslag nodig.

Het eerste lid betreft de evenknie van artikel 6, tweede lid, van dit wetsvoorstel. Het bevat een grondslag voor de kennisinstelling om het adviesverzoek en de daarbij behorende relevante informatie – dat (indirecte) persoonsgegevens kan bevatten – aan de Minister van OCW te verstrekken.

Onderdelen a tot en met d van het tweede lid noemen de in artikel 6 reeds genoemde ministers van ministeries waarvan de vertegenwoordigers op structurele dan wel incidentele basis deelnemen aan het 'backoffice' van het Loket Kennisveiligheid. Hiermee wordt voor hen een grondslag gecreëerd om input op een adviesverzoek te leveren aan de Minister van OCW. Deze input kan (indirecte) persoonsgegevens bevatten. Voor een beschrijving van het soort informatie dat aan de Minister van OCW wordt verstrekt door de genoemde Ministers wordt verwezen naar de paragraaf omtrent Gegevensverwerkingen door de backoffice van het Loket in de Memorie van Toelichting. Onderdeel e biedt de grondslag om input te ontvangen van een vakminister op een adviesverzoek, zoals bijvoorbeeld de Minister van Volksgezondheid, Welzijn en Sport.

Het derde lid biedt evenals artikel 6, derde lid, van dit wetsvoorstel een grondslag om bij algemene maatregel van bestuur partijen toe te voegen die aan de Minister van OCW persoonsgegevens kunnen verstrekken. Zie hiervoor ook de artikelsgewijze toelichting op artikel 5.

Artikel 8. Bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard

Het eerste lid van artikel 8 bevat een grondslag voor de verwerking van een aantal bijzondere categorieën van persoonsgegevens. Enkel de categorieën van bijzondere persoonsgegevens die relevant zijn in het kader van onderhavig wetsvoorstel zijn genoemd. Het gaat hier bijvoorbeeld om gegevens waaruit politieke opvattingen of etnische afkomst kunnen blijken. Incidenteel zullen deze categorieën van gegevens worden verwerkt om te komen tot een advies aan de kennisinstelling met een gedegen risicobeoordeling. Het gaat in beginsel om indirect herleidbare bijzondere persoonsgegevens.

Op grond van artikel 9 van de AVG is verwerking van bijzondere persoonsgegevens verboden, tenzij deze verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. (Indirect) herleidbare bijzondere persoonsgegevens zullen enkel incidenteel worden verwerkt als voor een specifiek adviesverzoek deze verwerking niet kan worden weggelaten om te komen tot een gedegen advies.

Het tweede lid van artikel 8 bevat een grondslag voor de verwerking van persoonsgegevens van strafrechtelijke aard. Het gaat hierbij om een incidentele verwerking van dit soort persoonsgegevens, bijvoorbeeld omdat het Loket Kennisveiligheid in haar zoekslag voor een voorgelegde casus stuit op nieuwsberichten of andersoortige berichten die betrekking hebben op stafrechtelijke veroordelingen, strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hierbij kan gedacht worden aan berichtgeving over steekpenningen. Het Loket zal geen persoonsgericht onderzoek verrichten naar justitiële en politiële gegevens.

Artikel 9. Rechten van betrokkenen

Artikel 9, eerste lid, voorziet in de mogelijkheid om in concrete gevallen conform de voorwaarden die de AVG daaraan stelt de rechten van betrokkene te beperken. In voorkomend geval kan het nodig zijn om de rechten van betrokkenen op grond van de AVG in te perken indien dit noodzakelijk is op grond van de nationale veiligheid. Daarmee wordt aangesloten bij artikel 23, eerste lid, onderdeel a, van de AVG die voorziet in de mogelijkheid om bij Unierechtelijke of lidstaatrechtelijke wetgevingsmaatregel die op de verwerkingsverantwoordelijke of de verwerker van toepassing is bepaalde rechten van betrokkene te beperken, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van een van de aldaar genoemde belangen. In dit geval is reeds gespecificeerd dat het gaat om het belang van de nationale veiligheid. In artikel 41 UAVG wordt invulling gegeven aan de ruimte die artikel 23 van de AVG biedt.

Het tweede lid bevat een nadere concretisering van de mogelijkheid de rechten van betrokkenen onder de AVG in te perken, waarbij de voorwaarde is opgenomen dat bij gebruikmaking van deze bevoegdheid moet worden voorzien in een dragende onderbouwing, die schriftelijk wordt medegedeeld aan de betrokkene wiens rechten worden beperkt.

Op grond van het derde lid kan een mededeling aan de betrokkene als bedoeld in het tweede lid achterwege worden gelaten indien dit afbreuk doet aan het doel van de beperking, in dit geval het belang van de nationale veiligheid.

Omdat het Loket kennisveiligheid in beginsel enkel indirecte persoonsgegevens verwerkt is het daarnaast belangrijk om te overwegen dat het altijd een grotere inbreuk op het privéleven van de betrokkene behelst om zijn rechten te effecturen. Daarnaast zal dit soms niet mogelijk zijn. De medewerkers van het Loket kennisveiligheid weten immers niet wiens persoonsgegevens zij verwerken en zullen bij een verzoek onder de AVG altijd een inspanning moeten verrichten om de indirecte persoonsgegevens direct te koppelen aan de betrokkene. Dit moet worden gewogen bij de beoordeling om al dan niet te voldoen aan een verzoek van een betrokkene.

Artikel 10. Evaluatiebepaling

Na twee jaar wordt de wet geëvalueerd. Een verslag daarvan wordt naar de Staten-Generaal gestuurd. In de evaluatie wordt in ieder geval een aantal elementen geadresseerd, waaronder het tijdelijke karakter van de wet. Er is gekozen voor een relatief korte evaluatieperiode, omdat gelijktijdig aan het creëren van deze wettelijke grondslag voor de gegevensverwerking van het Loket, er een evaluatie plaatsvindt van het Loket. Onder andere om na te gaan in hoe het Loket ook in de toekomst de kennisinstellingen zo goed mogelijk kan ondersteunen bij het weerbaarder maken van de wetenschap en het hoger onderwijs. Deze evaluatie zal uitwijzen of het wenselijk en nodig is om de advisering door het Loket permanent in te bedden.

Artikel 11. Inwerkingtreding

Artikel 10 regelt de inwerkingtreding, met hierbij de mogelijkheid van gefaseerde inwerkingtreding. Dit artikel bevat ook een zogenoemde ‘horizonbepaling'. Zie het slot van hoofdstuk 1 van het algemeen deel van de memorie van toelichting voor de onderbouwing hiervan.

De Minister van Onderwijs, Cultuur en Wetenschap,

Rianne Letschert