Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Cluster secretaris-generaal
Directie Europese en Internationale Aangelegenheden Europese Unie

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum
12 februari 2026

Onze referentie
-

Bijlage(n)
1

nota

Bijlage(n)

1. BNC-fiche Simplficatie NIS2-richtlijn
2. BNC-fiche Herziening Cybersecurity Act

1. Aanleiding

Op 20 januari 2026 heeft de Europese Commissie twee voorstellen gepubliceerd tot (1) simplificatie van de NIS2-richtlijn en (2) de herziening van de Cybersecurity Act. De voorstellen zijn gepubliceerd in de context van een verslechterd cyberdreigingslandschap, toenemende geopolitieke spanningen en groeiende digitale afhankelijkheden. Daarnaast is het Europese cybersecuritykader de afgelopen jaren sterk uitgebreid, wat heeft geleid tot een complex en deels gefragmenteerd regelgevingslandschap.

Met de herziening van de Cybersecurity Act beoogt de Commissie de Europese samenwerking en governance op het gebied van cybersecurity te versterken, de rol van het EU-agentschap ENISA te verduidelijken en uit te breiden, het Europese certificeringskader effectiever te maken en risico's in ICT-toeleveringsketens beter te adresseren. Certificering houdt in dat producten, diensten of organisaties een Europees veiligheidskeurmerk kunnen krijgen wanneer zij voldoen aan vastgestelde cybersecurity-eisen, zodat naleving van Europese verplichtingen eenvoudiger en uniformer kan worden aangetoond.

De vereenvoudiging van de NIS2-richtlijn beoogt de naleving te vereenvoudigen en een gestroomlijnde en coherente implementatie te waarborgen van specifieke aspecten van het cybersecuritykader**,** Beide voorstellen zijn er daarmee op gericht de digitale weerbaarheid van de Unie te versterken, een gelijk speelveld binnen de interne markt te waarborgen en de economische veiligheid van de EU te beschermen.

De fiches zijn geschreven in nauwe samenwerking met het ministerie van Economische Zaken en worden ook voorgelegd aan de minister van Economische Zaken. Op dit moment wordt door EZ gewerkt aan de appreciatie van de juridische appreciatie van de uitvoeringshandelingen in het fiche over de CSA, dit wordt z.s.m. aangepast.

2. Geadviseerd besluit

U wordt geadviseerd akkoord te geven op de BNC-fiches.

Cluster secretaris-generaal
Directie Europese en Internationale Aangelegenheden
Europese Unie

Datum
12 februari 2026

Onze referentie
-

3. Kernpunten

NIS2-richtlijn

- De Commissie beoogt met dit voorstel het cyberbeveiligingsniveau in de Europese Unie te versterken en te harmoniseren door consistentere regels vast te stellen, het toepassingsgebied te verbreden, de voorbereiding op en reactie bij cyberdreigingen te verbeteren en de samenwerking tussen lidstaten te versterken.
- Het voorstel wordt positief ontvangen en het kabinet onderkent de noodzaak van stevige Europese samenwerking op het gebied van digitale veiligheid en ondersteunt harmonisatie binnen de EU en de daaraan gerelateerde simplificatie van wetgeving op dit gebied. Dit voorstel sluit tevens aan bij de inzet van het kabinet ten behoeve van digitale weerbaarheid.

Cybersecurity Act

- Het voorstel tot herziening van de Cybersecurity Act introduceert een versterkt en uitgebreid mandaat voor ENISA, een hervormd en verbreed Europees cybersecuritycertificeringskader en een nieuw EU-raamwerk voor de veiligheid van ICT-toeleveringsketens. ENISA krijgt meer taken op het gebied van operationele samenwerking, incidentmanagement, certificering en capaciteitsopbouw. Het certificeringskader wordt uitgebreid naar de cyberweerbaarheid van entiteiten en sterker gekoppeld aan naleving van EU-wetgeving. Daarnaast wordt een mechanisme geïntroduceerd om hoog-risico leveranciers in kritieke ICT-ketens te identificeren en, indien nodig, bindende mitigerende maatregelen of uitsluitingen op te leggen.
- Het kabinet verwelkomt de doelstelling van de Commissie om de weerbaarheid van de EU te bevorderen middels het voorstel. Het kabinet benadrukt dat ENISA geen operationele taken toebedeeld dient te krijgen die raken aan nationale competenties of overlappen met bestaande nationale structuren en dienstverlening. Daarom kijkt het kabinet kritisch naar het opzetten van een 'early alert' helpdesk door ENISA. Dit overlapt namelijk met de dienstverlening van nationale structuren.

4. Toelichting

<u>Proces</u>

- Na bespreking in de ambtelijke voorportalen (de BNC op 18 februari en de CoCo op 24 februari), wordt het fiche naar verwachting ter instemming aangeboden aan de MR van 27 februari 2026 en daarna naar de Kamer verzonden.
- Verdere behandeling van het voorstel verloopt via de Telecom Raad

<u>ATR-advisering</u>

- Sinds 1 januari 2026 adviseert het ATR de Minister die het aangaat over de regeldrukeffecten van een ontwerp van een EU wetgevingshandeling waarvan de Minister die het aangaat een beoordeling maakt vanwege het belang van dat ontwerp voor Nederland.
- Het ATR heeft in het advies kritiek geuit op de informatieverstrekking door JenV ten behoeve van de ATR-advisering in dit BNC-proces.
- Het is van belang om te weten dat er een verschil van inzicht bestaat over de vraag of de regeldrukparagraaf of het gehele BNC-fiche met het ATR moet

worden gedeeld. De wet, ministeriële regeling en de bijbehorende toelichtingen geven hierover niet eenduidig uitsluitsel. Het delen van het hele fiche met het ATR voordat de interdepartementale afstemmingsrondes hebben plaatsgevonden is lastig werkbaar, omdat het ingewikkeld is om in zo een vroeg stadium een goed onderbouwd fiche tot stand te brengen. Daarnaast is het onwenselijk dat het ATR zich voor de advisering buigt over de inhoud aan informatie en kabinetsoordelen die in een later stadium van het BNC-proces achterhaald of beter onderbouwd kan zijn.
- EZ treedt in overleg met onder meer het ATR om ervoor te zorgen dat er duidelijke afspraken komen tussen de departementen en het ATR.

<u>Beoordeling NIS2-richtlijn</u>

- Het kabinet staat positief tegenover het voorstel dat aansluit op de verdere versterking van de digitale weerbaarheid binnen de EU.
- Het kabinet zal erop toezien dat de inhoud van het voorstel niet op gespannen voet komt te staan met in het bijzonder de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van de nationale veiligheid.
- Het kabinet beoordeelt de subsidiariteitstoets positief, Vanwege de hoge mate van verwevenheid van digitale processen binnen de EU en de grensoverschrijdende gevolgen van incidenten is een gemeenschappelijke aanpak voor een hoog gemeenschappelijk niveau van cyberbeveiliging noodzakelijk, waarbij optreden op EU-niveau passend en noodzakelijk is.
- Het oordeel van het kabinet op de proportionaliteitstoets is positief met enkele kanttekeningen. Deze kanttekeningen hebben met name betrekking op (i) de uitbreiding van het register bij ENISA, (ii) de voorgestelde wijziging die de lidstaten de mogelijkheid ontzegt om in geval van een uitvoeringshandeling aanvullende eisen te stellen aan de maatregelen in het kader van de zorgplicht, en (iii) de beperking van de auditbevoegdheden bij belangrijke entiteiten.

<u>Beoordeling CSA</u>

- Het kabinet staat overwegend positief tegenover de doelstelling om de Europese weerbaarheid en het gelijke speelveld in de interne markt te versterken. Tegelijkertijd plaatst het kabinet kanttekeningen bij mogelijke overlap van ENISA met nationale bevoegdheden, met name waar het operationele taken en incidentcommunicatie betreft. Ook is het kabinet kritisch op vergaande centralisatie en generieke landenaanwijzingen binnen het supply chain-raamwerk en benadrukt het belang van een risicogebaseerde, juridisch houdbare en proportionele toepassing, met voldoende betrokkenheid van lidstaten.
- Ten aanzien van de bevoegdheid oordeelt het kabinet positief: het voorstel is gebaseerd op artikel 114 VWEU en valt onder de gedeelde bevoegdheid inzake de interne markt. Ook het subsidiariteitsoordeel is positief, gezien het grensoverschrijdende karakter van cyberdreigingen en de noodzaak van een geharmoniseerde aanpak binnen de interne markt, met de kanttekening dat operationele samenwerking primair een nationale aangelegenheid blijft.
- Wat betreft proportionaliteit is het kabinet in beginsel positief: versterking van ENISA en het certificeringskader zijn geschikte middelen om de Europese cyberweerbaarheid te verhogen. Wel benadrukt het kabinet dat

overlap met bestaande nationale en Europese structuren moet worden voorkomen, dat maatregelen binnen het supply chain-raamwerk evenredig en uitvoerbaar moeten zijn, en dat rechtsbescherming en lidstaatinvloed adequaat moeten worden geborgd.

Cluster secretaris-generaal
Directie Europese en Internationale Aangelegenheden Europese Unie

Datum
12 februari 2026

Onze referentie
-

5. Informatie die niet openbaar gemaakt kan worden

5.1. Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer. Voor het overige is geen informatie opgenomen in de nota die niet openbaar gemaakt kan worden.