Raad van de Europese Unie

Brussel, 22 januari 2026
(OR. en)

Interinstitutionele dossiers:
2026/0011 (COD)
2026/0012 (COD)

5611/26
ADD 2

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	21 januari 2026
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	SWD(2026) 12 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG bij Voorstel voor een verordening van het Europees Parlement en de Raad betreffende het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees kader voor cyberbeveiligingscertificering, en de beveiliging van ICT-toeleveringsketens, en tot intrekking van Verordening (EU) 2019/881 (de cyberbeveiligingsverordening 2) en Voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2022/2555 betreffende vereenvoudigingsmaatregelen en afstemming op het [voorstel voor de cyberbeveiligingsverordening 2] […]

De delegaties vinden hierbij document SWD(2026) 12 final.

Bijlage: SWD(2026) 12 final

EUROPESE
COMMISSIE

Straatsburg, 20.1.2026
SWD(2026) 12 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG

bij

Voorstel voor een verordening van het Europees Parlement en de Raad betreffende het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees kader voor cyberbeveiligingscertificering, en de beveiliging van ICT-toeleveringsketens, en tot intrekking van Verordening (EU) 2019/881 (de cyberbeveiligingsverordening 2)

en

Voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2022/2555 betreffende vereenvoudigingsmaatregelen en afstemming op het [voorstel voor de cyberbeveiligingsverordening 2]

[…]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Samenvatting van de effectbeoordeling

Doelstelling

Het hoofddoel van deze effectbeoordeling is na te gaan of de huidige regelgeving toereikend is om veranderende cyberdreigingen in de hele EU aan te pakken. In de beoordeling wordt een geïntegreerde reeks beleidsopties voorgesteld om het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) te versterken, het Europees kader voor cyberbeveiligingscertificering (ECCF) te hervormen en de naleving van het bestaande wetgevingskader voor cyberbeveiliging te vereenvoudigen. Deze beoordeling onderstreept dat het van belang is cybergovernance af te stemmen op de technologische vooruitgang en de marktvraag, en tegelijkertijd het concurrentievermogen te waarborgen en rekening te houden met de milieueffecten.

Probleemstelling

Ondanks de lopende inspanningen heeft het cyberbeveiligingslandschap van de EU nog altijd te kampen met aanzienlijke uitdagingen in een context van steeds complexere dreigingen. Ontoereikende samenwerking tussen de lidstaten en andere actoren op EU-niveau hebben de uitvoering van beleidsinstrumenten doen stagneren, en regelgevende obstakels en complexiteit vormen een belemmering voor een efficiënt beheer van cyberbeveiliging. Deze problemen leiden tot hogere kosten voor bedrijven en overheidsinstanties, verhoogde risico's op cyberincidenten en inconsistente niveaus van bescherming voor burgers.

Rechtvaardiging van optreden op EU-niveau

Cyberdreigingen hebben een grensoverschrijdend karakter en een uniforme aanpak is dan ook van essentieel belang voor een krachtige respons. Optreden op EU-niveau zorgt voor consistente bescherming, vergroot het concurrentievermogen door te zorgen voor een gelijk speelveld en vergemakkelijkt het vrije verkeer van digitale diensten en producten binnen de eengemaakte markt. Harmonisatie op EU-niveau vermindert voorts de administratieve lasten door middel van vereenvoudigde naleving en gestroomlijnde procedures.

Beleidsopties en voorkeursoptie

In dit verslag worden vier actiegebieden geanalyseerd, elk met een reeks beleidsopties die in overweging worden genomen met het oog op de specifieke te verwezenlijken doelstellingen: (1) het Enisa-mandaat (ook onderdeel van de huidige cyberbeveiligingsverordening); (2) het ECCF (ook onderdeel van de huidige cyberbeveiligingsverordening), en (3) gerichte wijzigingen van de NIS2-richtlijn die gericht zijn op vereenvoudiging en ook verband houden met het Enisa-mandaat en het ECCF. Deze reeksen opties zijn op zichzelf al actiegebieden, maar zijn ook onderling verbonden en hebben betrekking op elkaar.

Opties om de incongruentie tussen het EU-beleidskader voor cyberbeveiliging en de behoeften van belanghebbenden in een steeds vijandigere omgeving aan te pakken

Optie A.1: *Verduidelijking van het Enisa-mandaat en prioritering* — Deze optie zou een duidelijk en stabiel kader voor de taken van Enisa waarborgen door de in andere wetgeving uiteengezette taken hierin op te nemen.

Optie A.2: *Hervorming van het Enisa-mandaat* — Deze optie zou leiden tot intrekking en vervanging van de cyberbeveiligingsverordening, met een herziening van het mandaat van het Agentschap tot gevolg.

Optie A.3: *Hervorming van het Enisa-mandaat met een sterke focus op operationele ondersteuning* — Deze optie zou voortbouwen op optie A.2. Daarnaast zou Enisa capaciteiten ontwikkelen om onder de NIS 2-richtlijn vallende entiteiten op verzoek van een lidstaat rechtstreeks te ondersteunen bij de respons op en het herstel van cyberbeveiligingsincidenten.

Opties betreffende het Europees kader voor cyberbeveiligingscertificering

Optie B.1: *Verduidelijking van het toepassingsgebied, de elementen en de doelstellingen van het ECCF en de invoering van een instandhoudingsmechanisme* — Deze optie voorziet in een nieuw instandhoudingsmechanisme voor de regelingen, na de vaststelling ervan, dat door Enisa moet worden toegepast.

Optie B.2: *Hervorming van het ECCF door herziening van de procedures ervan en uitbreiding van het toepassingsgebied met het oog op vereenvoudigde naleving van de regelgeving* — Met deze optie zou de cyberbeveiligingsverordening worden ingetrokken en worden vervangen door een nieuwe verordening. Naast optie B.1 zou de procedure voor het aanvragen, ontwikkelen en vaststellen van regelingen worden herzien om de verantwoordingsplicht en efficiëntie te verbeteren.

Optie B.3: *Hervorming van het ECCF zoals voorzien in optie B.2 en invoering van verplichte certificering met betrekking tot de cyberbeveiligingspositie* — Deze optie zou voortbouwen op optie B.2, maar heeft tot doel het effect van het kader verder te versterken door verplichte certificering in te voeren voor essentiële entiteiten die onder de NIS2-richtlijn vallen, rekening houdend met specifieke risicoscenario's, in plaats van uitsluitend te vertrouwen op vrijwillige certificering van entiteiten.

Opties betreffende vereenvoudiging

Optie C.1: *Hantering van een benadering op basis van zachte wetgeving en niet-wetgevingsinstrumenten, met inbegrip van het gebruik van bestaande bevoegdheden (vaststelling van uitvoeringshandelingen op grond van artikel 21, lid 5, en artikel 23, lid 11, van de NIS2-richtlijn)* — Deze optie voorziet in de vaststelling van uitvoeringshandelingen in het kader van de bestaande bevoegdheden uit hoofde van de NIS2-richtlijn om te zorgen voor een hogere mate van harmonisatie van de maatregelen voor het beheer van cyberbeveiligingsrisico's, van de drempels voor het melden van incidenten, alsook van informatie, vormen en procedures voor meldingen, in combinatie met de vaststelling van een reeks richtsnoeren ter vergroting van de rechtszekerheid en geharmoniseerde uitvoering.

Optie C.2: *Gerichte interventie — verdere vereenvoudiging van de naleving van het relevante wetgevingskader van de Unie inzake cyberbeveiliging* — Deze optie omvat beperkte

interventie door middel van wijzigingen van de cyberbeveiligingsverordening en de NIS2-richtlijn die gericht zijn op de vereenvoudiging van specifieke aspecten van het cyberbeveiligingskader, met inbegrip van aanpassingen van het toepassingsgebied, maximale harmonisatie voor uitvoeringshandelingen, bewijs van naleving door middel van certificering en de vaststelling van de reeks richtsnoeren als bedoeld in optie C1.

Optie C.3: *Harmonisatie van in de Uniewetgeving vastgestelde maatregelen op het gebied van cyberbeveiliging* — Deze optie zou voortbouwen op optie C.2 en hiermee zouden alle maatregelen of bevoegdheden voor het beheer van cyberbeveiligingsrisico's met betrekking tot die welke in sectorale wetgeving zijn opgenomen, worden geschrapt. In plaats daarvan zou het ecosysteem van de NIS2-richtlijn worden gewijzigd om te voorzien in gestroomlijnde vereisten voor alle soorten entiteiten, teneinde een hoger niveau van harmonisatie te waarborgen.

Opties betreffende de beveiliging van ICT-toeleveringsketens

Optie D.1: *Hantering van een benadering op basis van zachte wetgeving voor het aanpakken van cyberbeveiligingsrisico's voor ICT-toeleveringsketens* — Deze optie zou niet voorzien in regelgevend optreden op EU-niveau. In plaats daarvan zou de Commissie het aantal gecoördineerde risicobeoordelingen en vrijwillige instrumentaria verhogen.

Optie D.2: *Regelgevend optreden op ad-hocbasis met het oog op het codificeren van het 5G-instrumentarium* — Met deze optie zouden de maatregelen van het 5G-instrumentarium worden gecodificeerd. Deze optie zou de lidstaten ertoe verplichten ervoor te zorgen dat componenten van leveranciers met een hoog risico niet worden gebruikt in belangrijke activa van het netwerk.

Optie D.3: *Een alomvattend en horizontaal kader voor het aanpakken van cyberbeveiligingsrisico's in ICT-toeleveringsketens* — Deze optie zou voorzien in de totstandbrenging van een horizontaal, technologieneutraal en niet-sectorgebonden regelgevingskader voor het aanpakken van niet-technische cyberbeveiligingsrisico's in ICT-toeleveringsketens.

Na uitvoering van uitgebreide analyses omvat het voorkeursbeleidspakket: Optie A.2 — hervorming van het Enisa-mandaat; Optie B.2 — hervorming van het ECCF door herziening van de procedure en uitbreiding van het toepassingsgebied met het oog op vereenvoudigde naleving van de regelgeving, Optie C.2 — Gerichte interventie — verdere vereenvoudiging van de naleving van het relevante wetgevingskader van de Unie voor cyberbeveiliging, en Optie D.3 — een alomvattend en horizontaal kader voor het aanpakken van cyberbeveiligingsrisico's in ICT-toeleveringsketens.

Deze combinatie biedt een evenwichtig antwoord op vastgestelde beleidsuitdagingen en doet de doeltreffendheid, efficiëntie en samenhang in de hele EU aanzienlijk toenemen.

Belangrijkste effecten

Kosten-batenanalyse: de overgang naar het voorgestelde regelgevingskader zal kosten met zich meebrengen, zowel voor Enisa, in de vorm van naar schatting 161,3 miljoen EUR over een periode van vijf jaar voor het vervullen van zijn nieuwe taken, als voor overheidsinstanties in de hele EU, in de vorm van naar schatting 80 miljoen EUR voor toezicht (rekening houdend met de relevante kostenbesparingen). Wat bedrijven betreft zou de uitfasering van specifieke apparatuur met een hoog risico tijdens een overgangsperiode van drie jaar kunnen leiden tot jaarlijkse kosten van 3,4 tot 4,3 miljard EUR voor exploitanten van mobiele netwerken, terwijl de investeringen in betrouwbare leveranciers tegelijkertijd met wel 2 miljard EUR per jaar zouden kunnen toenemen. Bovendien zullen gestroomlijnde en verminderde nalevingsverplichtingen voor bedrijven naar verwachting leiden tot kostenbesparingen tot 14,6 miljard EUR. Daarnaast zouden de verbetering van de algemene cyberbeveiligingspositie en technologische soevereiniteit van de EU en het stimuleren van innovatie en concurrentievermogen aanzienlijke voordelen voor burgers, overheidsinstanties en bedrijven met zich brengen, die naar verwachting de initiële uitgaven op den duur grotendeels zullen compenseren.

Concurrentievermogen: door de versnippering van de markt terug te dringen en de regelgeving te harmoniseren, komen de voorkeursopties de eerlijke concurrentie in de hele EU ten goede en bieden zij bedrijven een duidelijkere koers richting naleving en innovatie.

Klimaatconsistentiecontrole: bij de beoordeling werd rekening gehouden met de potentiële milieueffecten van elke optie. Er werd bijzondere aandacht besteed aan energie-efficiëntie, door reizen veroorzaakte emissies en de consolidering van de infrastructuur. De voorkeursopties A.2, B.2 en C.2 hebben een beperkt milieueffect, terwijl optie D.3 gebaseerd is op milieuneutraliteit, rekening houdend met de levenscyclus van producten en overgangsperioden voor de vervanging van belangrijke activa. Dit strookt met het EU-streven naar duurzaamheid.

Digitaal by default: de nadruk op gestroomlijnde digitale processen toont aan dat de EU zich inzet voor een "digitaal eerst"-aanpak die zorgt voor een snellere en betrouwbaardere gegevensuitwisseling en besluitvorming. Optie D.3 zou ook grote gevolgen kunnen hebben voor de digitalisering, aangezien deze optie gepaard gaat met de vervanging van componenten van entiteiten die gevestigd zijn in of onder zeggenschap staan van entiteiten uit derde landen die aanleiding geven tot bezorgdheid over cyberbeveiliging.

Vereenvoudiging en lastenverlichting: de voorkeursopties dragen bij tot vereenvoudiging door verduidelijkingen met betrekking tot het toepassingsgebied en door maatregelen om de naleving en het toezicht te stroomlijnen, met een vermindering van de administratieve lasten tot gevolg. Er wordt rekening gehouden met het "one in, one out"-beginsel door ervoor te zorgen dat nieuwe verplichtingen worden gecompenseerd door verlagingen elders.

Conclusie

Deze effectbeoordeling voorziet in een alomvattende strategie om de cyberbeveiliging van de EU te verbeteren, inefficiënties op het gebied van regelgeving aan te pakken en het digitale landschap voor te bereiden op toekomstige uitdagingen. De beoordeling bevat een

aanbeveling voor een aanpak op basis van samenwerking en samenhang, waarbij beleidshervormingen berusten op bestaande kaders en tegelijkertijd wordt voorzien in een aanpassing aan de nieuwe technologische realiteit. Met deze maatregelen beoogt de EU een weerbare, concurrerende en duurzame digitale economie te waarborgen.