



EUROPESE
COMMISSIE

Brussel, 3.6.2026
COM(2026) 502 final

2026/0138 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

**tot vaststelling van een kader van maatregelen ter versterking van het Europese cloud-
en AI-ecosysteem (verordening cloud- en AI-ontwikkeling)**

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

(Voor de EER relevante tekst)

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

De afgelopen jaren zijn cloud- en AI-technologieën, -diensten en -toepassingen uitgegroeid van nieuwe concepten tot onmisbare pijlers waarop het functioneren van onze economie en samenleving rust. Artificiële intelligentie (AI) biedt ongekennde mogelijkheden, variërend van automatisering en gegevensgestuurde besluitvorming tot gepersonaliseerde diensten, terwijl cloudcomputing de computingmiddelen, softwarebouwstenen en interfaces levert die nodig zijn voor een efficiënte ontwikkeling en inzet van AI. De snelle opmars van AI heeft geleid tot een ongekennde en steeds grotere vraag naar computingcapaciteiten. Bijgevolg is computinginfrastructuur niet langer louter een technisch activum, maar is deze uitgegroeid tot een strategisch middel dat cruciaal is voor de economische veiligheid, soevereiniteit, weerbaarheid en concurrentiekracht van de Unie.

Zoals Mario Draghi in zijn rapport “De toekomst van het Europese concurrentievermogen” stelt, moet de EU haar positie behouden op gebieden waar technologische soevereiniteit vereist is, zoals beveiliging en encryptie (“soevereine cloud”-oplossingen), en zo kritieke externe afhankelijkheid verminderen door de eigen cloud- en AI-capaciteiten en -infrastructuur te versterken. Daartoe wordt de Europese Commissie in het rapport-Draghi opgeroepen om gerichte maatregelen te nemen die ernaar streven de zeggenschap over gegevens en cloudcomputingdiensten terug te winnen en te behouden, de binnenlandse computingcapaciteit uit te breiden en een robuust financieel en talentcirculatiesysteem op te zetten om innovatie te stimuleren.

Deze doelstellingen werden later vastgelegd in het Europese actieplan voor het AI-continent, dat een strategische routekaart bevatte om het Europese leiderschap op het gebied van artificiële intelligentie te waarborgen. Om dit te bereiken is een samenhang tussen vijf belangrijke domeinen cruciaal: computinginfrastructuur, gegevens, vaardigheden, de ontwikkeling en invoering van AI-algoritmen, en vereenvoudiging van de regelgeving. De lopende uitrol van AI-fabrieken en AI-gigafabrieken heeft tot doel Europese bedrijven en onderzoekers die behoefte hebben aan AI-capaciteiten, brede toegang te bieden tot computingmiddelen van de volgende generatie met een hoge capaciteit. Om dit aan te vullen, moet de EU haar cloud- en datacentrumcapaciteit uitbreiden om de bredere inzet en verspreiding van AI te ondersteunen.

De beperkte capaciteit van de datacentra van de Unie vormt een aanzienlijke bedreiging voor haar vermogen om te profiteren van de digitale transformatie en op AI gebaseerde oplossingen in te voeren, met name oplossingen die computingcapaciteit met een lage latentie vereisen. Er zijn met name verschillende belemmeringen die de snelle ingebruikname van datacentra in de EU in de weg staan. Naarmate de vraag naar gegevensopslag en -verwerking blijft toenemen, met name als gevolg van de sterke stijging van AI-werkbelastingen, dwingt het gebrek aan datacentrumcapaciteit in de EU Europese ondernemingen ertoe om kritieke werkbelastingen via de infrastructuur van buitenlandse hyperscalers te laten lopen. Hierdoor is de EU een minder aantrekkelijke bestemming voor investeringen in technologie dan regio's met ruimere en goedkopere computingmiddelen.

Het huidige landschap op het gebied van cloud en AI wordt gekenmerkt door een **uitgesproken afhankelijkheid van een beperkt aantal aanbieders uit derde landen**. Hoewel de EU-markt voor cloudcomputingdiensten aanzienlijk groeit, is het marktaandeel van EU-aanbieders gedaald van 29 % in 2017 tot 15 % in 2022 en is het sindsdien stabiel gebleven.

Momenteel hebben drie hyperscalers van buiten de EU meer dan 70 % van de Europese cloudmarkt in handen. Grote gevestigde partijen vallen onder de jurisdictie van derde landen waar wetten met extraterritoriale werking van toepassing zijn, waaronder wetten die de toegang tot en overdracht van gegevens voorschrijven en die mogelijk in strijd zijn met de grondrechten en de kaders voor gegevensbescherming van de EU. Deze afhankelijkheid stelt Europese gebruikers ook bloot aan de risico's die verband houden met een onderbreking van de dienstverlening, met name in scenario's waarin eenzijdige beslissingen van actoren uit derde landen de dienstverlening zouden kunnen verstoren.

Europa beschikt weliswaar over onderzoeks- en ontwikkelingscapaciteiten van wereldklasse, levendige opensourcegemeenschappen en een sterke industriële basis op het gebied van cloud en AI, maar deze blijven nog grotendeels onbenut.

Tegen deze achtergrond heeft de Commissie het **voorstel voor een verordening cloud- en AI-ontwikkeling** ("het voorstel") opgesteld, dat tot doel heeft de beperkte en geografisch geconcentreerde beschikbaarheid van computingcapaciteit in de EU aan te pakken, evenals de risico's die gepaard gaan met de afhankelijkheid van cloud- en AI-diensten die door niet-Europese aanbieders worden geleverd. Met het voorstel wordt beoogd:

- 1) de in de EU ingezette computingcapaciteit en de in de EU ontwikkelde en ingezette AI te vergroten door middel van innovatieve en duurzame cloud- en AI-technologieën;
- 2) te zorgen voor aantrekkelijke voorwaarden voor de inzet van duurzame en innovatieve computingcapaciteit in de hele Unie;
- 3) aandacht te besteden aan zorgen over gegevenssoevereiniteit en operationele continuïteit van cloud en AI;
- 4) de openbare orde te beschermen door de weerbaarheid van de levering van cloudcomputingdiensten te vergroten, met name in de publieke sector.

Met het voorstel wordt ingespeeld op de behoefte aan een gecoördineerde "ecosysteembenadering" om de EU op het gebied van cloud en AI concurrerder en weerbaarder te maken. In het voorstel worden maatregelen aan de aanbodzijde om de binnenlandse capaciteiten te versterken, gecombineerd met maatregelen aan de vraagzijde om de acceptatie te stimuleren en met faciliterende maatregelen om innovatie en investeringen in cloud en AI te bevorderen. Er wordt specifiek de nadruk gelegd op opensource als hefboom om de technologische soevereiniteit te versterken, in overeenstemming met de EU-opensourcestrategie, die tot doel heeft open Europese alternatieven binnen de gehele Europese technologiestack te bevorderen.

Ten eerste worden in het voorstel projecten ondersteund die voortvloeien uit het onderzoeks- en innovatie-initiatief dat in dit kader is gelanceerd en gezamenlijk met de lidstaten wordt uitgevoerd. Dit initiatief zal netwerken, de cloud, AI en software integreren in samenhangende ecosystemen om de volgende punten aan te pakken:

- 1) toekomstige uitdagingen op het gebied van energie-efficiënte computinginfrastructuur;
- 2) autonomie in de gehele cloudstack;
- 3) geavanceerde EU-capaciteiten op het gebied van geavanceerde AI-technologieën, zoals grensverleggende AI, fysieke AI en industriële AI;
- 4) de invoering van cloudtechnologie en AI in zowel de publieke als de private sector.

In het voorstel wordt in het bijzonder nadruk gelegd op grootschalige, sectoroverschrijdende initiatieven die gericht zijn op de meest strategische technologische en industriële uitdagingen (“grote uitdagingen”). Het zal de haalbaarheid van deze initiatieven aantonen en de weg vrijmaken voor soortgelijke initiatieven in de toekomst, waardoor de voorwaarden worden geschapen voor investeringen in infrastructuur en technologieën van de volgende generatie.

Ten tweede bevat het voorstel een reactie op de groeiende kloof in de capaciteit van datacentra door middel van een kader dat de ingebruikname van datacentra in de hele EU vereenvoudigt en harmoniseert, en tegelijkertijd de duurzaamheid ervan waarborgt. Het doel is om de capaciteit van de EU in de komende vijf tot zeven jaar te verdrievoudigen en tegen 2035 de benodigde capaciteit te bereiken, waarbij gezorgd wordt voor een evenwichtige geografische spreiding over de lidstaten. Ter ondersteuning hiervan wordt in het voorstel een mechanisme voorgesteld om strategische datacentrumprojecten te identificeren en te ondersteunen die een aanzienlijke mate van ingebouwde innovatie en duurzaamheid bevatten of die bijdragen aan een evenwichtige verdeling van de computingcapaciteit.

Ten derde beoogt het voorstel de risico's te beperken die voortvloeien uit de afhankelijkheid van de EU van derde landen voor cloudcomputingdiensten, door middel van één enkel, EU-breed kader voor soevereiniteit. Het voorstel voorziet in een geharmoniseerde en controleerbare reeks criteria op verschillende soevereiniteitsniveaus van cloudcomputingdiensten. Het biedt tevens een kader voor de beoordeling en formele erkenning van diensten op een bepaald soevereiniteitsniveau. Ten slotte verplicht worden de lidstaten er in het voorstel toe verplicht om soevereiniteitsrisicobeoordelingen uit te voeren om vast te stellen voor welke subsectoren en gebruiksscenario's diensten moeten worden aangeboden die zijn afgestemd op de respectieve soevereiniteitsniveaus, teneinde een passende bescherming te waarborgen op het gebied van gegevensvertrouwelijkheid, operationele autonomie te waarborgen en schade te voorkomen die de openbare orde zou kunnen ondermijnen.

Het voorstel vormt een aanvulling op de **herziening van de cyberbeveiligingsverordening (CSA2)**, die betrekking heeft op risico's in de toeleveringsketen, en zorgt ervoor dat aanbestedende diensten gebruik kunnen maken van soevereine cloudcomputingdiensten. Het voorstel en de CSA2 pakken samen de al lang bestaande lacunes op het gebied van soevereiniteit en niet-technische risico's aan. Tegelijkertijd moeten cloudcomputingdiensten in Europa voldoen aan strenge normen op het gebied van cyberbeveiliging, wat vraagt om een robuust cyberbeveiligingskader dat een alomvattend antwoord biedt op de huidige geopolitieke beveiligingsuitdagingen. In deze wetgevingscontext zullen de werkzaamheden worden hervat met betrekking tot de **Europese cyberbeveiligingscertificeringsregeling voor clouddiensten (EUCS)**.

Het voorstel biedt aanbestedende diensten tot slot een kader om weloverwogen aankoopbeslissingen te nemen en hun koopkracht in te zetten om bestaande afhankelijkheden te verminderen, onder meer door gebruik te maken van sectorspecifieke gunningscriteria met EU-meerwaarde en gezamenlijke aanbestedingen om innovatie en groei te stimuleren, waarbij de nadruk ligt op het creëren van concrete kansen voor kleinere, in de EU gevestigde aanbieders.

Al met al leggen de in het voorstel uiteengezette maatregelen de basis voor een weerbaar en hoogwaardig EU-ecosysteem op het gebied van cloud en AI. Zij positioneren Europa niet alleen als afnemer van geavanceerde digitale technologieën, maar ook als mondiaal knooppunt voor betrouwbare, soevereine en schaalbare digitale infrastructuur die in staat is om de normen, capaciteiten en markten van de volgende technologische golf vorm te geven.

- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Het voorstel is in overeenstemming met de regels inzake het overstappen naar een andere dataverwerkingsdienst die zijn ingevoerd bij de **dataverordening**. Door het mogelijk te maken om van aanbieder te wisselen en belangrijke oorzaken van de afhankelijkheid van één aanbieder weg te nemen, beoogt de dataverordening ervoor te zorgen dat aanbieders van cloudcomputingdiensten in de EU met elkaar concurreren op het gebied van kwaliteit, innovatie en prijs. Het doel is om cloudegebruikers in staat te stellen vrij te kiezen welke aanbieder het beste aan hun behoeften voldoet en het aanbod van verschillende aanbieders te combineren in een multicloudbenadering.

De dataverordening bevat echter geen bepalingen om het aanbod van Europese cloudcomputingdiensten concurrerender te maken of om de toetreding tot de markt van een grotere verscheidenheid aan aanbieders van cloudcomputingdiensten te stimuleren.

De dataverordening maakt de weg vrij voor een mogelijke vermindering van de afhankelijkheid van aanbieders van buiten de EU, maar legt niet de basis voor een meer soevereine en betrouwbare cloudcomputingsector in de EU. Dankzij de bepalingen inzake het overstappen naar andere clouddiensten en interoperabiliteit kunnen gebruikers echter in grotere mate gebruikmaken van Europese cloudcomputingdiensten. De dataverordening maakt dit voorstel derhalve mogelijk.

Het voorstel sluit ook aan bij de **digitaalemarktenverordening**. In de digitaalemarktenverordening komen cloudcomputingdiensten als een kernplatformdienst aan bod, wat inhoudt dat aanbieders van cloudcomputingdiensten die als poortwachter zijn aangemerkt, aan een reeks verplichtingen moeten voldoen om de eerlijkheid en de betwistbaarheid van de markt te bevorderen. Tot nu toe is er nog geen aanbieder van cloudcomputingdiensten aangewezen als poortwachter voor zijn diensten. Op 18 november 2025 heeft de Commissie echter in het kader van de digitaalemarktenverordening drie marktonderzoeken ingesteld naar cloudcomputingdiensten. In twee van deze marktonderzoeken zal worden onderzocht of twee aanbieders moeten worden aangewezen als poortwachters voor hun cloudcomputingdiensten (met andere woorden: of zij voor zakelijke gebruikers een belangrijke toegangspoort tot eindgebruikers vormen). In het derde marktonderzoek zal worden onderzocht of de digitaalemarktenverordening op doeltreffende wijze een einde kan maken aan praktijken die de concurrentie en de eerlijkheid in de cloudcomputingsector in de EU kunnen beperken.

Hoewel bepaalde aanbieders van cloudcomputingdiensten zowel in het kader van dit voorstel als in het kader van de digitaalemarktenverordening zouden kunnen worden gereguleerd, heeft de digitaalemarktenverordening andere doelstellingen en bevat deze geen maatregelen die het gebruik van soevereine cloudcomputingdiensten actief zouden bevorderen. De digitaalemarktenverordening is uitsluitend bedoeld om een eerlijke en betwistbare cloudmarkt in de Unie in stand te houden en te bevorderen, door specifieke gedragingen van als poortwachter aangewezen ondernemingen te reguleren, en grijpt daarmee in op een ander niveau dan het voorstel, dat zich richt op de acceptatie en het gebruik van de aangeboden diensten.

Het voorstel versterkt tevens de belangrijkste doelstellingen van de **AI-verordening**. In de AI-verordening worden de regels voor AI-systemen en AI-modellen voor algemene doeleinden die op de EU-markt worden gebracht geharmoniseerd, waardoor de werking van de interne markt wordt verbeterd en de invoering van mensgerichte en betrouwbare AI in de hele waardeketen wordt bevorderd. De AI-verordening waarborgt een hoog niveau van bescherming van gezondheid, veiligheid en de grondrechten. Het heeft geen betrekking op aspecten van soevereiniteit.

Het voorstel vormt bovendien een aanvulling op het bredere beleidskader van de EU op digitaal gebied, waaronder de **EU-opensourcestrategie**, het **beleidsprogramma voor het digitale decennium** en de **AI-toepassingsstrategie**.

In de **EU-opensourcestrategie** wordt voorgesteld om opensource te bevorderen met het oog op soevereiniteit, concurrentievermogen en beveiliging door middel van een reeks gerichte maatregelen, waarvan sommige worden voorgesteld in de verordening cloud- en AI-ontwikkeling.

Het **beleidsprogramma voor het digitale decennium** richt zich op vier hoofdpunten, waaronder de doelstellingen vallen, namelijk i) een digitaal vaardige bevolking en hooggekwalificeerde digitale professionals, ii) veilige en duurzame digitale infrastructuur, iii) digitale transformatie van bedrijven en iv) digitalisering van overheidsdiensten. Meer in het bijzonder bevat het beleidsprogramma voor het digitale decennium een streefcijfer voor het monitoren van de uitrol van edge nodes, maar het bevat noch een streefcijfer voor het meten van de voortgang bij de uitrol van computingcapaciteit of datacentra in de EU, noch concrete ondersteunende maatregelen voor de uitrol daarvan. Dit voorstel vormt een aanvulling op het beleidsprogramma voor het digitale decennium door gebruik te maken van de bestaande jaarlijkse monitoring, waardoor synergieën met het bestaande kader worden gecreëerd. Het draagt ook bij aan de verwezenlijking van alle vier de hoofddoelstellingen van het beleidsprogramma voor het digitale decennium, met name door concrete maatregelen vast te stellen die gericht zijn op de ontwikkeling van innovatieve op AI gebaseerde technologieën, de inzet van uitgebreide computingcapaciteit en het creëren van een vertrouwenskader voor een intensiever gebruik van cloud en AI.

Bovendien worden in de **AI-toepassingsstrategie** concrete maatregelen uiteengezet om het transformatieve potentieel van AI te benutten, waarbij de nadruk ligt op het stimuleren van de toepassing ervan in belangrijke industriële sectoren en de publieke sector. Daarnaast worden er ondersteunende maatregelen geïntroduceerd om de technologische soevereiniteit van de EU te versterken door sectoroverschrijdende uitdagingen op het gebied van de ontwikkeling en toepassing van AI aan te pakken. Het voorstel ondersteunt deze doelstellingen en draagt bij aan de verwezenlijking ervan door specifieke maatregelen in te voeren die gericht zijn op het ondersteunen van de ontwikkeling en invoering van cloud en AI, het vergroten van de toegang tot computingcapaciteit en het opbouwen van vertrouwen in cloudcomputingdiensten.

Het voorstel sluit volledig aan bij de **mededeling over een internationale digitale strategie** van de EU van juni 2025. Het biedt een transparant en niet-discriminerend kader voor digitale autonomie, waardoor binnen de EU weerbare en soevereine technologische infrastructuur kan worden opgebouwd en tegelijkertijd een betrouwbaar, juridisch solide model kan worden geboden voor internationale partnerschappen en multilaterale governance buiten de EU. Dit is volledig in overeenstemming met de internationale verbintenissen en partnerschappen van de Unie en zal entiteiten uit partnerlanden die voldoen aan de vereiste waarborgniveaus van de Unie, toegang tot de interne markt garanderen.

- **Verenigbaarheid met andere beleidsterreinen van de Unie**

Het voorstel vormt een aanvulling op het bredere beleidskader van de EU inzake cyberbeveiliging en digitale weerbaarheid.

Dit voorstel moet worden gelezen in samenhang met het voorstel voor de herziening van de **chipsverordening**, dat maatregelen bevat om investeringen in geavanceerde halfgeleiders te stimuleren, de weerbaarheid van de toeleveringsketen te vergroten en de vraag te stimuleren door middel van intensievere samenwerking tussen de toeleveringsketen voor halfgeleiders en de eindmarkten.

De **richtlijn beveiliging van netwerk- en informatiesystemen (NIS 2-richtlijn)** zorgt voor een beter risicobeheer op het gebied van cyberbeveiliging bij aanbieders van cloudcomputingdiensten en datacentra in de EU, wat leidt tot meer vertrouwen. Die richtlijn bevat echter geen maatregelen om de acceptatie en het gebruik van dergelijke diensten te stimuleren en is volledig gericht op technische cyberbeveiliging, in tegenstelling tot bredere soevereiniteitsoverwegingen.

Zoals eerder uiteengezet, wordt in het voorstel de nadruk die in de **cyberbeveiligingsverordening** ligt op cyberbeveiliging in de cloud, verder aangevuld met overwegingen op het gebied van soevereiniteit. Certificering op grond van de cyberbeveiligingsverordening kan betrekking hebben op technische criteria op het gebied van cyberbeveiliging, maar is niet geschikt om soevereiniteitskwesties aan te pakken die verder gaan dan deze technische aspecten. Ondertussen werkt het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) aan de ontwikkeling van een **Europese cyberbeveiligingscertificeringsregeling voor clouddiensten (EUCS)**, die nog niet is vastgesteld. Zodra die regeling definitief is vastgesteld, zou deze kunnen worden ingezet binnen het kader voor soevereine cloudcomputingdiensten om te waarborgen dat een gecontroleerde dienst voldoet aan de hoogste normen op het gebied van cyberbeveiliging. Bovendien versterkt de voorgestelde herziening van de cyberbeveiligingsverordening de betrouwbaarheid van de ICT-toeleveringsketen voor hardware en software.

Het voorstel sluit ook aan bij de doelstellingen van de **verordening digitale operationele weerbaarheid (DORA-verordening)**. In de DORA-verordening zijn de nalegingsverplichtingen vastgesteld voor aanbieders van cloudcomputingdiensten. De regeling is indirect van toepassing op aanbieders van cloudcomputingdiensten indien zij diensten verlenen aan bepaalde financiële entiteiten of indien hun rol vanuit het oogpunt van operationele weerbaarheid voldoende belangrijk is. De verordening heeft een sectorale reikwijdte en is specifiek gericht op de financiële sector. Op grond van de DORA-verordening moeten aanbieders van cloudcomputingdiensten ICT-risicobeheer invoeren en regelmatig tests ten aanzien van incidentrespons uitvoeren om te voldoen aan de eisen die gelden voor kritieke externe dienstverleners. De betrokken financiële instellingen, die van openbare aard kunnen zijn, moeten een zorgvuldig onderzoek (due diligence) uitvoeren naar de aanbieders van cloudcomputingdiensten waarmee zij samenwerken.

Het voorstel sluit ook aan bij de doelstellingen van de **strategie voor een paraatheidsunie**, waarin de afhankelijkheid van kritieke digitale infrastructuur als een systeemrisico wordt aangemerkt en wordt opgeroepen tot een overheidsbrede aanpak om de continuïteit van essentiële diensten in crisissituaties te waarborgen. Het bij deze verordening vastgestelde soevereiniteitskader, en met name het risicobeoordelingsmechanisme van artikel 29, draagt rechtstreeks bij aan de digitale paraatheidsdimensie van die strategie door te waarborgen dat de cloud- en AI-diensten die ten grondslag liggen aan het beheer van noodsituaties, de coördinatie van de civiele bescherming en rampenbestrijdingsoperaties, worden geleverd op het passende Uniebetrouwbaarheidsniveau. Het voorstel sluit derhalve aan bij de bredere beleidsdoelstellingen van de Unie op het gebied van weerbaarheid en paraatheid en draagt hieraan bij.

Het voorstel is in overeenstemming met de bestaande regels inzake de verwerking van persoonsgegevens, waaronder de **algemene verordening gegevensbescherming (AVG)** en het EU-VS-kader voor gegevensbescherming. Hoewel het EU-VS-kader voor gegevensbescherming betrekking heeft op trans-Atlantische gegevensoverdracht, neemt het de bezorgdheid over soevereiniteit in verband met de afhankelijkheid van dienstverleners uit derde landen echter niet weg. Het voorstel vormt dus een aanvulling op het EU-VS-kader

voor gegevensbescherming, aangezien het begrip soevereiniteit verder reikt dan gegevensoverdracht en ook betrekking heeft op operationele autonomie.

Het voorstel vormt tevens een aanvulling op de **richtlijnen inzake overheidsopdrachten**. Overheidsinstanties in de EU zijn in hoge mate afhankelijk van aanbieders van cloudcomputingdiensten van buiten de EU, en de daarmee samenhangende problemen vragen om een genuanceerde en gerichte sectorale aanpak, die niet onder de bestaande richtlijnen inzake overheidsopdrachten valt en waar een overkoepelende aanpak onvoldoende recht aan zou doen. Het voorstel biedt derhalve een sectorspecifieke benadering van soevereiniteit, waarvan de vele facetten niet aan bod kunnen komen in het horizontale acquis waarin algemene beginselen voor de opzet van aanbestedingsprocedures zijn vastgelegd. Het voorstel bevat aanvullende gunningscriteria die eveneens zijn afgestemd op de specifieke kenmerken van cloudcomputingdiensten en de kritieke afhankelijkheden van derde landen in deze sector.

Het voorstel vormt een aanvulling op de **digitalenetwerkenverordening**, waarin de ontwikkeling van robuuste, snelle, veilige en geavanceerde digitale netwerken wordt ondersteund en die daarmee een positieve bijdrage levert aan de uitrol van datacentra in de EU, waarvoor supersnelle connectiviteit op gigabit-niveau en daarboven een eerste vereiste is. In het voorstel wordt gebruikgemaakt van de vooruitgang die de digitalenetwerkenverordening op het gebied van connectiviteit heeft gebracht en blijft daarmee gericht op de uitrol van datacentrumcapaciteit, en niet op de voorafgaande of gelijktijdige aanleg van de benodigde connectiviteitsinfrastructuur. De digitalenetwerkenverordening heeft ook betrekking op de convergentie van netwerkinfrastructuur, zoals situaties waarin een aanbieder van cloudcomputingdiensten een elektronisch communicatienetwerk exploiteert en tot nu toe niet onderworpen was aan de verplichtingen uit hoofde van het **Europese wetboek voor elektronische communicatie**, ondanks dat deze wel onder het toepassingsgebied daarvan valt. De digitalenetwerkenverordening zal dus duidelijkheid scheppen over de procedures voor connectiviteit tussen aanbieders van verschillende netwerken en andere marktdeelnemers in het kader van een bredere samenwerking binnen het ecosysteem.

Het voorstel draagt bij aan de doelstellingen van de **richtlijn energie-efficiëntie** om de datacentrumsector aan te zetten tot grotere energie-efficiëntie. Afgezien van overwegingen op het gebied van transparantie en reputatie biedt de richtlijn echter geen stimulansen voor exploitanten van datacentra om hun prestaties op het gebied van duurzaamheid te verbeteren, en bevat deze geen maatregelen om de uitrol van duurzame datacentra in de hele EU te versnellen of de daarmee samenhangende investeringen te vergroten.

Evenzo heeft de **EU-gedragscode inzake energie-efficiëntie in datacentra** geen betrekking op maatregelen voor de ingebruikname van een datacentrum, maar richt deze zich volledig op werkwijzen voor de exploitatie ervan. Het voorstel bevat dan ook maatregelen om de uitrol van energie-efficiënte datacentra te stimuleren, in lijn met de **strategische routekaart voor digitalisering en AI in de energiesector**, die tot doel heeft het energieverbruik van digitale technologieën te optimaliseren en tegelijkertijd de groene en de digitale transitie van de EU te versnellen. Om vast te stellen welke datacentra duurzaam zijn, wordt in het voorstel verwezen naar de beoordelingsregeling die in het kader van de richtlijn energie-efficiëntie is ontwikkeld.

Het voorstel vormt tevens een aanvulling op het **pakket Europese netten**, dat tot doel heeft ervoor te zorgen dat de netten aanwezig en klaar zijn om toekomstige belasting op horizontale wijze op te vangen. In dit voorstel ligt de nadruk op datacentra als eindafnemers van netcapaciteit en wordt ervoor gezorgd dat bij de locatiekeuze van datacentra rekening wordt gehouden met de beschikbaarheid van het net, dat er ruim van tevoren informatie wordt

uitgewisseld zodat deze kan worden meegenomen in de netplanning en dat daarmee een tijdige aansluiting van datacentra wordt gewaarborgd.

In het pakket Europese netten worden manieren beschreven waarop lidstaten netaansluitingen kunnen versnellen, onder meer door hun wachtrij voor netaansluitingen efficiënter in te richten, bijvoorbeeld door rekening te houden met de gereedheid van een project en de netvriendelijkheid van het gebruik, in plaats van uitsluitend uit te gaan van de “wie het eerst komt, het eerst maalt”-aanpak. In het voorstel wordt rekening gehouden met deze overwegingen.

Het voorstel vormt tevens een aanvulling op de **richtlijn hernieuwbare energie** en kan daarop voortbouwen. Datacentra kunnen profiteren van de toegenomen beschikbaarheid van hernieuwbare energie en opslagcapaciteit, ook al vallen ze zelf niet onder de richtlijn. De nabijheid van gebieden voor de versnelde uitrol van hernieuwbare energie zou ook een relevante factor kunnen zijn bij het aanwijzen van locaties voor een snellere uitrol van datacentra.

De **verordening industriële versnelling** bevat maatregelen om de vergunningverlening te versnellen, waaronder de vastlegging van het principe “één project, één procedure” en de instelling van één digitale procedure die de gehele vergunningprocedure omvat. In de verordening industriële versnelling wordt tevens voorgeschreven dat de lidstaten ten minste één gebied of cluster voor versnelde industriële productie moeten aanwijzen waar aanvullende maatregelen ter facilitering van bedrijfsactiviteiten van toepassing zijn, waaronder voorrang bij de toegang tot materialen en toegang tot EU-financiering. Aangezien de voorgestelde maatregelen voor industriële versnelling echter alleen betrekking hebben op productiefaciliteiten en geen rekening houden met de specifieke behoeften van datacentra en de voordelen die deze bieden, vallen ze buiten het toepassingsgebied van de verordening industriële versnelling. Om deze verschillen aan te pakken, vormt het voorstel een aanvulling op de algemene maatregelen voor industriële versnelling met behulp van maatregelen die specifiek zijn afgestemd op de versnelde uitrol van datacentra.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De rechtsgrondslag voor dit voorstel is **artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU)**, dat de EU de bevoegdheid verleent maatregelen vast te stellen ter verbetering van de werking van de interne markt door middel van de harmonisatie van nationale bepalingen.

De huidige versnippering bij de uitrol van datacentra wordt veroorzaakt door uiteenlopende nationale benaderingen op het gebied van capaciteitsuitbreiding, duurzaamheidseisen en vergunningsprocedures. Deze risico's leiden tot verschillen in regelgeving die de interne markt zouden kunnen ondermijnen.

Verschillen in de praktijken op het gebied van overheidsopdrachten voor cloudcomputingdiensten, evenals inconsistente soevereiniteitscriteria, kunnen het voor aanbieders moeilijker maken om naadloos in alle lidstaten actief te zijn, wat kan leiden tot marktinefficiënties en ongelijke concurrentievoorwaarden.

Gezien deze uitdagingen is een maatregel op EU-niveau in de vorm van een wetsvoorstel gerechtvaardigd op grond van artikel 114 VWEU, aangezien deze tot doel heeft belemmeringen voor de interne markt weg te nemen en gelijke concurrentievoorwaarden te creëren voor aanbieders van cloudcomputingdiensten.

Daarnaast is het voorstel mede gebaseerd op **artikel 173, lid 3, VWEU**, dat de rechtsgrondslag vormt voor maatregelen die gericht zijn op het versterken van het industriële concurrentievermogen en de innovatiecapaciteit van de EU. Het huidige tekort aan computingcapaciteit in de EU beperkt het vermogen van de Europese industrie om ten volle te profiteren van het gebruik van cloud- en AI-technologieën, met name die waarvoor een lage latentie en high-performance computing vereist zijn. Door de beschikbaarheid van energie-efficiënte computingcapaciteit te vergroten en door middel van de ontwikkeling en implementatie van geavanceerde cloud- en AI-technologieën draagt dit initiatief rechtstreeks bij aan de versterking van het industriële concurrentievermogen en het technologisch leiderschap van Europa, in overeenstemming met de doelstellingen van artikel 173, lid 3, VWEU.

Gezien de tweeledige doelstelling van het voorstel, namelijk het verhelpen van verstoringen van de interne markt en het versterken van het industriële concurrentievermogen van de EU, zal het worden vastgesteld als één enkel wetgevingsinstrument op basis van de cumulatieve rechtsgrondslag van artikel 114 en artikel 173, lid 3, VWEU. Deze gezamenlijke rechtsgrondslag biedt een eenduidig regelgevingskader voor de onderling samenhangende uitdagingen van marktversnippering en de opbouw van strategische industriële capaciteit binnen het cloud- en AI-ecosysteem van de EU.

- **Subsidiariteit (bij niet-exclusieve bevoegdheid)**

Maatregelen van de EU bieden een duidelijke meerwaarde bij het aanpakken van het probleem van de beperkte en geografisch geconcentreerde beschikbaarheid van computingcapaciteit. Door een gemeenschappelijke aanpak te bieden voor het versnellen van de uitrol van datacentra, maken de maatregelen een samenhangende planning en inzet van computingcapaciteit op een geografisch evenwichtige manier mogelijk, terwijl een “race to the bottom” wordt voorkomen en de regelgevingscomplexiteit voor investeerders en exploitanten van datacentra wordt verminderd.

De EU bevindt zich in een unieke positie om ervoor te zorgen dat het investerings- en versnellingsbeleid aansluit bij de gezamenlijke prioriteiten en versnippering voorkomt. Maatregelen op EU-niveau zouden ervoor zorgen dat alle bedrijven en overheidsinstanties toegang hebben tot voldoende computingcapaciteit om aan hun behoeften te voldoen, en vormen een voorwaarde om van Europa een AI-continent te maken.

Door de afhankelijkheid van cloudcomputingdiensten van niet-Europese aanbieders aan te pakken, leveren de maatregelen van de EU voordelen op die verder gaan dan wat de lidstaten afzonderlijk zouden kunnen bereiken, met name bij het aanpakken van de onderliggende markttekortkomingen als gevolg van onvolledige informatie. Dit zal de werking van de interne markt verbeteren en aanbieders van cloudcomputingdiensten in staat stellen om ook buiten hun nationale markten te groeien.

- **Evenredigheid**

In het voorstel wordt een gerichte en evenredige aanpak gehanteerd om de kritieke knelpunten in de eengemaakte markt aan te pakken, met name het tekort aan computingcapaciteit en de te grote afhankelijkheid van aanbieders uit derde landen. De voorgestelde oplossingen beperken zich tot maatregelen die essentieel zijn voor het bereiken van de kerndoelstellingen van het voorstel, met name het versterken van de technologische soevereiniteit van de EU, het bevorderen van een concurrerende EU-markt voor clouddiensten en artificiële intelligentie, en het ondersteunen van een betere beschikbaarheid van duurzame computingmiddelen in de EU.

Door de nadruk te leggen op geharmoniseerde normen voor soevereine cloudcomputingdiensten, een gestroomlijnde uitrol van datacentra en EU-brede

samenwerkingsmechanismen, wordt overmatige regelgeving met het voorstel voorkomen en worden tegelijkertijd in heel Europa de structurele belemmeringen aangepakt die de digitale vooruitgang in de weg staan. De gekozen maatregelen vormen de meest geschikte en minst ingrijpende manier om de vastgestelde markt- en regelgevingstekortkomingen aan te pakken, aangezien zij gebruikmaken van bestaande EU-instrumenten en tegelijkertijd alleen die nieuwe bepalingen invoeren die nodig zijn voor een samenhangende en efficiënte uitvoering.

Het voorstel brengt directe nalevingskosten met zich mee, die zowel administratieve als aanpassingsuitgaven omvatten. Deze kosten komen hoofdzakelijk ten laste van nationale en lokale overheidsinstanties, en van bedrijven zoals exploitanten van datacentra, aanbieders van cloudcomputingdiensten, alsmede hun onderaannemers en entiteiten uit de particuliere sector die actief zijn in de sectoren die zijn opgenomen in bijlage I bij de NIS 2-richtlijn, zodat zij voldoen aan de in deze verordening vastgestelde verplichtingen.

Op basis van de verkenning van verschillende opties en de verwachte kosten en baten is een uitgebalanceerd instrument ontwikkeld. De kosten voor overheidsinstanties zullen worden gecompenseerd door de besparingen op de totale eigendomskosten van IT-systemen en door snellere en betrouwbaardere aanbestedingsprocessen, terwijl de kosten voor bedrijven zullen worden gecompenseerd door de verbeterde voorspelbaarheid van de regelgevingskoers, de verminderde versnippering van nationale benaderingen en de vereenvoudiging van de administratieve procedures.

- **Keuze van het instrument**

De Commissie stelt een verordening voor als het meest geschikte rechtsinstrument om de doelstellingen van het voorstel te verwezenlijken, aangezien een verordening een uniforme toepassing en onmiddellijke werking in alle lidstaten waarborgt. Een verordening biedt de nodige rechtszekerheid en consistentie om het regelgevingskader voor cloudcomputingdiensten volledig te harmoniseren. Deze aanpak is essentieel om belemmeringen voor de eengemaakte markt weg te nemen, met name op gebieden zoals soevereiniteit en duurzaamheidsnormen, waar uiteenlopende nationale regels anders de technologische soevereiniteit en het concurrentievermogen van de EU zouden kunnen ondermijnen. Gezien de geopolitieke urgentie, waaronder de noodzaak om de strategische afhankelijkheid van aanbieders uit derde landen te verminderen, zorgt een verordening voor een snelle, gecoördineerde en EU-brede reactie, waardoor vertragingen of inconsistenties worden voorkomen die zouden kunnen ontstaan als lidstaten onafhankelijker zouden handelen.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Raadpleging van belanghebbenden**

Tussen oktober 2024 en november 2025 vond een uitgebreide raadpleging van belanghebbenden plaats, bestaande uit de volgende raadplegingsactiviteiten.

Tussen april en juli 2025 heeft de Commissie een openbare raadpleging georganiseerd, bestaande uit een onlinevragenlijst en een verzoek om input, waarbij belanghebbenden gedetailleerde standpuntnota's konden indienen waarin zij hun standpunten en aanbevelingen over de doelstellingen en de in het voorstel beoogde maatregelen uiteenzetten, en tegelijkertijd rechtstreeks bewijsmateriaal konden aanleveren ter onderbouwing van de uitwerking van beleidsopties. In totaal kwamen er 436 reacties binnen: 243 voor de raadplegingsvragenlijst en 193 voor het verzoek om input.

De raadpleging werd aangevuld met een reeks workshops, seminars en rondetafelgesprekken. Deze omvatten: i) de 6e algemene vergadering en het alliantieforum van de Europese alliantie voor industriële gegevens, edge en cloud; ii) rondetafelgesprekken, en wel over investeringen in cloudcomputing met financiële investeerders, over beleidsmaatregelen om de integratie van datacentra in het EU-net te vergemakkelijken, met directieleden van Europese aanbieders van clouddiensten over de ontwikkeling van soeverein cloudaanbod in de EU, en met de Amerikaanse kamer van koophandel; iii) seminars met vertegenwoordigers uit het bedrijfsleven, de academische wereld en overheidsinstanties over de economische dynamiek van de AI-stack en iv) presentaties over het toekomstige EU-beleid inzake cloud en AI met het bedrijfsleven.

De Commissie heeft tevens een voortdurende dialoog onderhouden met de relevante autoriteiten van de lidstaten, die bijeen zijn gekomen in de informele cloudsamenwerkingsgroep van de lidstaten in het kader van de Europese alliantie voor industriële gegevens, edge en cloud, aangevuld met gerichte bilaterale bijeenkomsten.

Daarnaast heeft de Commissie verdere bilaterale besprekingen gevoerd met derde landen, waaronder Japan, Zwitserland en het Verenigd Koninkrijk, om de overwogen beleidsopties te presenteren en te bespreken, en tegelijkertijd inzicht te vergaren in beste praktijken en de externe effecten van de overwogen maatregelen te beoordelen.

Ten slotte heeft de Commissie meer dan honderd bilaterale bijeenkomsten gehouden met een breed scala aan belanghebbenden, waaronder vertegenwoordigers van het bedrijfsleven, academische instellingen, denktanks en maatschappelijke organisaties, die hebben bijgedragen aan de uitwerking van de voorgestelde beleidsopties.

- **Bijeenbrengen en gebruik van expertise**

De Commissie heeft een consortium onder leiding van Technopolis Group ingeschakeld om een studie uit te voeren ter ondersteuning van de fase van het verzamelen en analyseren van bewijsmateriaal in het kader van de effectbeoordeling die aan het voorstel voorafgaat. In het kader van het onderzoek werden diverse activiteiten georganiseerd om belanghebbenden bij het proces te betrekken, waaronder meer dan 60 gerichte interviews, enquêtes (meer dan 250 reacties) en workshops (meer dan 100 deelnemers).

- **Effectbeoordeling**

Het voorstel gaat vergezeld van een uitgebreide effectbeoordeling, waarvan de definitieve versie op 30 april 2026 aan de Raad voor regelgevingstoetsing is voorgelegd. Op 8 mei 2026 heeft de raad een positief advies uitgebracht, vergezeld van een verzoek om verdere verbeteringen.

- **Grondrechten**

Het voorstel is onderworpen aan een uitgebreide beoordeling van de gevolgen ervan voor de grondrechten, waarbij bijzondere aandacht is besteed aan de bescherming van persoonsgegevens zoals gewaarborgd in artikel 8 van het Handvest van de grondrechten van de Europese Unie. Met het voorstel wordt een kader ingevoerd voor soevereine cloudcomputingdiensten, waarin strenge waarborgen zijn vastgelegd om ervoor te zorgen dat de verwerking van persoonsgegevens van EU-burgers voldoet aan de EU-normen inzake gegevensbescherming, waaronder de AVG. Door deze normen vast te stellen, beperkt het voorstel de risico's die gepaard gaan met het niet-conform omgaan met gegevens en versterkt het tegelijkertijd het vertrouwen in de digitale infrastructuur.

Een van de belangrijkste doelstellingen van het voorstel is het verminderen van de afhankelijkheid van aanbieders uit derde landen, wier activiteiten mogelijk onderworpen zijn

aan rechtsgebieden buiten de EU waar toegang tot en doorgifte van gegevens is toegestaan. Met het voorstel wordt de bescherming van persoonsgegevens dan ook versterkt door ervoor te zorgen dat deze gegevens onder effectief toezicht van de EU-autoriteiten blijven, waaronder de gegevensbeschermingsautoriteiten van de lidstaten en het Europees Comité voor gegevensbescherming. Deze aanpak vergroot de rechtszekerheid en waarborgt het recht op privacy zoals vastgelegd in het Handvest.

Bovendien bevordert het voorstel een concurrerende eengemaakte markt voor cloudcomputingdiensten, waarin aanbieders volledig gebonden zijn aan de EU-wetgeving en onderworpen zijn aan de geldende verplichtingen. Dit verbetert niet alleen de beschikbaarheid en continuïteit van gegevens, maar zorgt er ook voor dat consequent aan de wettelijke verplichtingen van de EU, zoals die met betrekking tot de rechten van betrokkenen en het toezicht door regelgevende instanties, wordt voldaan. Door de marktaanwezigheid van in de EU gevestigde aanbieders te versterken, wordt met het voorstel de bescherming van de grondrechten nog steviger verankerd in het digitale ecosysteem en worden betere waarborgen geboden tegen ongeoorloofde toegang tot of misbruik van persoonsgegevens. Er is zorgvuldig gekeken naar de evenredigheid van deze maatregelen om een evenwicht te vinden tussen innovatie en de noodzaak om rechten te beschermen, in overeenstemming met de beginselen van het Handvest.

4. GEVOLGEN VOOR DE BEGROTING

De gevolgen van het voorstel voor de begroting worden uitvoerig beschreven in het bijgevoegde financieel memorandum. Om het initiatief doeltreffend uit te voeren, zijn 25 voltijdsequivalenten (vte's) nodig, bestaande uit 9 vaste posten en 16 posten voor arbeidscontractanten. Deze personeelsbezetting zal worden gerealiseerd door een combinatie van herplaatsing en extra aanwerving. Concreet zullen 15 huidige medewerkers binnen de Commissie worden herplaatst om het initiatief te ondersteunen, waarbij gebruik wordt gemaakt van hun expertise en ervaring met het beheer van soortgelijke maatregelen. Het benodigde personeel zal afkomstig zijn van DG CNECT en DG DIGIT, waar zij momenteel bij de betreffende eenheden zijn ingedeeld, of zal vanuit de diensten van de Commissie worden heringedeeld. Ter aanvulling op deze bestaande middelen zijn voor het initiatief 10 extra vte's nodig: 6 vte's voor DG CNECT en 4 vte's voor DG DIGIT. Deze extra medewerkers zullen worden ingezet om de huidige personeelsbezetting te versterken, teneinde de succesvolle uitvoering van het initiatief en de effectieve uitvoering van nieuwe activiteiten en taken te waarborgen.

De extra administratieve uitgaven die gepaard gaan met de in het voorstel beschreven nieuwe taken zullen grotendeels worden gefinancierd uit inkomsten uit vergoedingen die onder de interne bestemmingsontvangsten vallen, waardoor wordt gezorgd voor een duurzaam en levensvatbaar financieringsmodel. Concreet zullen de inkomsten uit vergoedingen worden gebruikt ter ondersteuning van taken in verband met gezamenlijke aanbestedingen en het beheer van het EuroCloud-initiatief, dat tot doel heeft het voor geïnteresseerde lidstaten gemakkelijker te maken om onbenutte cloud- en datacentrumcapaciteit te delen.

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

De Commissie moet de toepassing van de voorgestelde verordening monitoren en de doeltreffendheid ervan in de loop van de tijd evalueren. Vijf jaar na de inwerkingtreding ervan zou de Commissie de uitvoering van deze voorgestelde verordening moeten evalueren en

daarover een verslag indienen bij het Europees Parlement en de Raad. Deze verslagen zijn openbaar en geven nadere toelichting over de daadwerkelijke toepassing en handhaving van de voorgestelde verordening.

- **Artikelsgewijze toelichting van de voorgestelde verordening**

Titel I van de voorgestelde verordening bevat de algemene bepalingen, waaronder het toepassingsgebied (artikel 1) en de definities (artikel 2).

Titel II bevat de bepalingen die het kader vormen voor de uitvoering van ontwikkelings- en uitrolactiviteiten binnen het cloud- en AI-ecosysteem. Het kader is onderverdeeld in de initiatieven voor cloud- en AI-leiderschap en wordt ondersteund door aanvullende maatregelen. In hoofdstuk I wordt in artikel 3 de algemene doelstelling van de initiatieven voor cloud- en AI-leiderschap uiteengezet, die erop gericht zijn onderzoeks- en innovatieactiviteiten te ondersteunen en grootschalige capaciteit te realiseren in het gehele cloud- en AI-ecosysteem van de Unie. In artikel 4 worden de operationele doelstellingen van de initiatieven voor cloud- en AI-leiderschap vastgelegd. Artikel 5 voorziet in de oprichting van een netwerk van ervarings- en versnellingscentra voor AI, dat voortbouwt op de Europese digitale-innovatiehubs en tot doel heeft de verwezenlijking van de doelstellingen van de initiatieven voor cloud- en AI-leiderschap te ondersteunen. In artikel 6 worden de uitvoeringsmechanismen voor de initiatieven voor cloud- en AI-leiderschap uiteengezet. In artikel 7 wordt voorgeschreven dat de lidstaten binnen een jaar na de inwerkingtreding van de verordening een nationale cloud- en AI-strategie moeten vaststellen die aansluit bij de doelstellingen van de verordening. In artikel 8 worden de criteria vastgesteld waaraan projecten moeten voldoen om door de Commissie te worden erkend als een prioritair project op het gebied van grensverleggende AI. Artikel 9 ondersteunt de toewijzing van AI-computingmiddelen aan prioritaire projecten op het gebied van grensverleggende AI, en ondersteunt tevens industriële en fysieke AI-projecten en de ontwikkeling en uitrol van AI-modellen voor de publieke sector.

In titel III worden de bepalingen inzake de capaciteit van datacentra vastgelegd. In hoofdstuk I worden in artikel 10 de verplichtingen voor de lidstaten vastgelegd om op hun grondgebied zones voor de versnelde uitrol van datacentra aan te wijzen, waar zij datacentrumcapaciteit aanleggen. In artikel 11 worden de voorwaarden binnen zones voor de versnelde uitrol van datacentra geregeld. Artikel 12 bevat de verplichting voor de lidstaten om centrale informatiepunten aan te wijzen of, waar mogelijk, de reeds bestaande centrale informatiepunten uit te breiden of hiermee te integreren, voor exploitanten van datacentrumprojecten in zones voor de versnelde uitrol van datacentra, en bevat voorts beginselen waaraan moet worden voldaan met betrekking tot de verantwoordelijkheden van het informatiepunt. Artikel 13 heeft betrekking op de vereenvoudigde administratieve procedures en vergunningsprocedures voor datacentrumprojecten die worden uitgevoerd in zones voor de versnelde uitrol van datacentra. In hoofdstuk II wordt in artikel 14 het mechanisme voor het indienen van blijken van belangstelling vastgelegd, evenals de voorwaarden voor en de aanwijzing door de Commissie van strategische datacentrumprojecten. In hoofdstuk III wordt in artikel 15 een mechanisme vastgesteld waarmee de Commissie toezicht kan houden op de vooruitgang die de Unie boekt bij het vergroten van de beschikbare computingcapaciteit, de omvang van de vraag naar datacentrumcapaciteit en de omvang van de capaciteitskloof.

Titel IV bevat de bepalingen inzake autonomie en vaststelling. In hoofdstuk I, afdeling 1, wordt in artikel 16 een Uniekader voor cloudcomputingsovereïniteit uiteengezet, dat bestaat uit vier betrouwbaarheidsniveaus, en worden de in bijlage II bij de verordening vastgestelde

vereisten ingevoerd waaraan cloudcomputingdiensten moeten voldoen om te worden beschouwd als diensten die een Uniebetrouwbaarheidsniveau van 1 tot en met 4 bieden. In artikel 17 wordt een mechanisme vastgesteld waarmee aanbieders van cloudcomputingdiensten kunnen worden erkend als aanbieders die voldoen aan Uniebetrouwbaarheidsniveau 1, 2, 3 of 4; zij moeten hiervoor een aanvraag tot erkenning indienen bij de nationale bevoegde autoriteit van vestiging. In artikel 18 worden de voorwaarden en een mechanisme vastgelegd voor een eventuele erkenning van derde landen als landen die voldoende betrouwbaarheid bieden, zodat cloudcomputingdiensten die vanuit dat derde land worden beheerd, in aanmerking kunnen komen voor Uniebetrouwbaarheidsniveau 3. In afdeling 2 worden in artikel 19 de voorwaarden uiteengezet voor de conformiteitszelfbeoordeling, waarbij wordt vastgelegd in hoeverre aan de vereisten van het Uniebetrouwbaarheidsniveau 1 wordt voldaan. In afdeling 3 wordt in artikel 20 het kader uiteengezet voor de beoordeling die door controleorganisaties wordt uitgevoerd aan de hand van de vereisten van de Uniebetrouwbaarheidsniveaus 2 tot en met 4. In artikel 21 worden de vereisten uiteengezet waaraan controlebewijs moet voldoen in het kader van de beoordeling door een derde partij van de vereisten op grond van de Uniebetrouwbaarheidsniveaus 2 tot en met 4. Artikel 22 bevat de verplichting voor de Commissie om een centraal register op te zetten en bij te houden van diensten die erkend zijn als diensten die de Uniebetrouwbaarheidsniveaus 1 tot en met 4 bieden. Artikel 23 bevat transparantieplichtingen voor aanbieders van cloudcomputingdiensten om melding te maken van alle essentiële wijzigingen die aanleiding kunnen geven tot een wijziging in hun erkenning als aanbieders die de Uniebetrouwbaarheidsniveaus 1 tot en met 4 bieden. In artikel 24 worden de sancties en de regels inzake compensatie vastgelegd die van toepassing zijn op inbreuken door aanbieders van cloudcomputingdiensten. In afdeling 4 worden in artikel 25 de verplichtingen van de lidstaten vastgelegd om een nationale bevoegde autoriteit aan te wijzen. In artikel 26 worden de bevoegdheden van de door de lidstaten aangewezen nationale bevoegde autoriteiten vastgesteld. In afdeling 5 worden in artikel 27 de beginselen vastgelegd voor wederzijdse bijstand tussen de nationale bevoegde autoriteiten van de lidstaten in het kader van informatie-uitwisseling en onderzoek ten behoeve van deze verordening. In artikel 28 worden de beginselen vastgelegd voor landsgrensoverschrijdende samenwerking tussen de nationale bevoegde autoriteiten van de lidstaten in het kader van handhavingsmaatregelen. In hoofdstuk II, afdeling 1, worden in artikel 29 de verplichtingen voor de lidstaten en de entiteiten van de Unie vastgelegd om risicobeoordelingen uit te voeren teneinde het vereiste conformiteitsniveau vast te stellen in het licht van de Uniebetrouwbaarheidsniveaus 2 tot en met 4 voor verschillende activiteiten in de publieke sector. In artikel 30 worden aanbestedende diensten die cloudcomputingdiensten aanschaffen de verplichting opgelegd om, als minimumvereiste, Uniebetrouwbaarheidsniveau 1 te vereisen. Indien uit een risicobeoordeling blijkt dat de activiteiten van dergelijke aanbestedende diensten van belang zijn voor de openbare orde, mogen zij uitsluitend diensten inkopen en gebruiken waarvan is erkend dat deze voldoen aan de Uniebetrouwbaarheidsniveaus 2, 3 of 4. In afdeling 2 wordt in artikel 31 toegestaan dat entiteiten uit de particuliere sector in de zin van de NIS 2-richtlijn effectbeoordelingen uitvoeren met een soortgelijk doel als die welke worden uitgevoerd door entiteiten van de Unie en openbare lichamen. In afdeling 3 worden in artikel 32 de verplichtingen vastgelegd voor de aanbestedende diensten van de lidstaten om bij overheidsopdrachten voor cloudcomputingdiensten en AI-systemen die binnen het toepassingsgebied van de verordening vallen, criteria inzake de meerwaarde van de Unie toe te passen. Artikel 33 bevat de verplichting voor de lidstaten om toezicht te houden op hun aanbestedingen op het gebied van innovatie van cloudcomputingdiensten en AI-systemen, wordt een gestroomlijnd rapportagekader ingevoerd en worden verbanden gelegd met nationale cloud- en AI-strategieën, waarbij de lidstaten plannen moeten opstellen om de doelstellingen van dit artikel

te verwezenlijken. In hoofdstuk III wordt bij artikel 34 de Europese cloudfederatie voor de publieke sector (“Federatie EuroCloud”) opgericht en worden het toepassingsgebied en het doel ervan vastgelegd. In artikel 35 worden de voorwaarden vastgelegd die van toepassing zijn op het gezamenlijk gebruik van datacentrumsdiensten en cloudcomputingdiensten binnen de Federatie EuroCloud. In artikel 36 wordt uiteengezet hoe de Commissie de kosten kan terugvorderen die zijn gemaakt in verband met de Federatie EuroCloud, waaronder de oprichting van de Federatie EuroCloud en van het platform dat de uitwisseling van diensten tussen de leden ervan mogelijk maakt. In hoofdstuk IV worden in artikel 37 de voorwaarden vastgelegd waaronder de Commissie aanbestedingsactiviteiten kan uitvoeren voor entiteiten van de Unie, voor aanbestedende diensten van de lidstaten en voor door de Commissie geselecteerde partnerorganisaties, onder meer door de nodige afwijkingen van het Financieel Reglement vast te stellen. In artikel 38 worden de nodige regelingen vastgelegd voor de uitvoering van het gemeenschappelijk aanbestedingskader, inclusief het governancemechanisme. In artikel 39 worden de toepasselijke regels inzake overheidsopdrachten vastgelegd. In artikel 40 wordt het mechanisme beschreven voor de compensatie van de kosten die de Commissie maakt voor het beheer van het gemeenschappelijk aanbestedingskader, door middel van vergoedingen die aan de deelnemende aanbestedende diensten in rekening worden gebracht. In hoofdstuk VI worden in artikel 41 de verplichtingen van de entiteiten van de Unie en openbare lichamen vastgelegd om het gebruik van opensourceoplossingen te bevorderen en te vergemakkelijken ten opzichte van door eigendomsrechten beschermde oplossingen. In artikel 42 worden de vereisten vastgelegd met betrekking tot het delen en hergebruiken van software die is ontwikkeld door of voor entiteiten van de Unie en openbare lichamen. Artikel 43 bevat de verplichting voor de Commissie om een catalogus van opensourceoplossingen op te stellen en bij te houden. In artikel 44 worden de regels vastgelegd voor de oprichting van een netwerk van opensourceprogrammabureaus van de lidstaten.

Titel V bevat de slotbepalingen, waaronder de bevoegdheid van de Commissie om gedelegeerde handelingen (artikel 45) en uitvoeringshandelingen (artikel 46) vast te stellen, de evaluatieclausule (artikel 47) en de bepalingen inzake de inwerkingtreding en de datums van toepassing van de verordening (artikel 48).

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot vaststelling van een kader van maatregelen ter versterking van het Europese cloud- en AI-ecosysteem (verordening cloud- en AI-ontwikkeling)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114 en artikel 173, lid 3,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité¹,

Gezien het advies van het Comité van de Regio's²,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

- (1) De Unie is vastbesloten om een wereldleider te worden op het gebied van artificiële intelligentie (AI). Door snellere innovatie, grotere efficiëntie en slimmere besluitvorming mogelijk te maken, draagt AI bij aan aanzienlijke economische, ecologische en maatschappelijke voordelen en vormt het een fundamentele aanjager van het concurrentievermogen. Om de voordelen van AI in de belangrijkste sectoren van de economie ten volle te benutten, moet de Unie ambitieus en vooruitziend handelen, haar innovatievermogen vergroten, haar concurrentievermogen en voorzieningszekerheid versterken en tegelijkertijd haar technologische soevereiniteit en strategische autonomie op het gebied van geavanceerde digitale technologieën versterken.
- (2) De Unie heeft al een stevige basis gelegd om Europa te positioneren als een continent dat vooroploopt op het gebied van de ontwikkeling en toepassing van AI, met name via de mededeling over het actieplan voor het AI-continent³ en de AI-toepassingsstrategie⁴. Door middel van Verordening (EU) 2023/2854 van het Europees Parlement en de Raad⁵ betreffende geharmoniseerde regels inzake eerlijke toegang tot

¹ PB C, , blz. .

² PB C, , blz. .

³ Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 9 april 2025, "Actieplan voor het AI-continent" ([COM\(2025\) 165 final](#)).

⁴ Mededeling van de Commissie aan het Europees Parlement en de Raad, "AI-toepassingsstrategie" (8.10.2025, [COM\(2025\) 723 final](#)).

⁵ Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot

en eerlijk gebruik van data (“de dataverordening”) en de Data Union Strategy⁶ (strategie voor een Europese data-unie), heeft de Unie tevens het noodzakelijke kader ingevoerd om een veilige en interoperabele eengemaakte markt voor gegevens tot stand te brengen, die de basis vormt voor de ontwikkeling van AI.

- (3) Het Europees Parlement, de Raad, de Commissie en de lidstaten hebben zich ertoe verbonden samen te werken om de technologische soevereiniteit van de Unie op een open manier te verwezenlijken, met name door middel van veilige en toegankelijke digitale en gegevensinfrastructuur die andere technologische ontwikkelingen mogelijk maakt, ter ondersteuning van het concurrentievermogen en de duurzaamheid van de industrie en de economie van de Unie (in het bijzonder van kleine en middelgrote ondernemingen (“kmo’s”)⁷ en kleine midcaps⁸) en van de weerbaarheid van de waardeketens van de Unie, alsook ter bevordering van het ecosysteem voor start-ups, onder meer door de soepele werking van de voormalige Europese digitale-innovatiehubs (“EDIH’s”), die zijn omgevormd tot ervarings- en versnellingscentra voor AI (“centra voor AI”).
- (4) De Unie is in toenemende mate afhankelijk geworden van een beperkt aantal aanbieders van cloudcomputingdiensten uit derde landen. Het versterken van de capaciteit van de Unie om cloud- en AI-technologieën op haar grondgebied te ontwikkelen en in te zetten, is een strategische prioriteit geworden voor het concurrentievermogen, de voorzieningszekerheid en de technologische soevereiniteit van de Unie, zoals benadrukt in het verslag van Mario Draghi over de toekomst van het Europese concurrentievermogen⁹ en in overeenstemming met de mededeling “Versterking van de economische veiligheid van de EU”¹⁰. Deze uitdagingen voor het cloud- en AI-ecosysteem van de Unie vragen om grootschalige technologische capaciteitsopbouw en ondersteuning op het gebied van onderzoeks- en innovatieactiviteiten, en vereisen een gezamenlijke inspanning van de lidstaten, waarbij de Unie de ontwikkeling en inzet van cloud- en AI-technologieën en van grootschalige cloudcomputingcapaciteit ondersteunt.
- (5) Die afhankelijkheid leidt niet alleen tot beperkte marktaandelen voor de Europese aanbieders van cloudcomputingdiensten, maar ook tot aanzienlijke risico’s voor de operationele autonomie, weerbaarheid en veiligheid van de Unie. De Raad heeft opgeroepen tot een verordening cloud- en AI-ontwikkeling, waarin gemeenschappelijke criteria voor soevereine cloudcomputingdiensten worden vastgelegd, zodat risico’s op het gebied van markttransparantie en risico’s in verband

wijziging van Verordening (EU) 2017/2394 en Richtlijn (EU) 2020/1828 (Dataverordening) (PB L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

⁶ Mededeling van de Commissie aan het Europees Parlement en de Raad, “Data Union Strategy” (19.11.2025, [COM\(2025\) 835 final](https://data.europa.eu/eli/reg/2025/835/oj)).

⁷ Zoals gedefinieerd in titel I, artikel 2, van de bijlage bij Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36, ELI: <http://data.europa.eu/eli/reco/2003/361/oj>).

⁸ Zoals gedefinieerd in punt 2 van de bijlage bij Aanbeveling (EU) 2025/1099 van de Commissie van 21 mei 2025 betreffende de definitie van kleine midcapondernemingen (PB L, 2025/1099, 28.5.2025, ELI: <http://data.europa.eu/eli/reco/2025/1099/oj>).

⁹ “The future of European competitiveness. Part A, A competitiveness strategy for Europe” (De toekomst van het Europese concurrentievermogen. Deel A, een strategie voor het concurrentievermogen van Europa) (“het rapport-Draghi”), september 2024 (<https://data.europa.eu/doi/10.2872/9356120>).

¹⁰ Gezamenlijke mededeling van de Commissie aan het Europees Parlement en de Raad, “Versterking van de economische veiligheid van de EU” ([JOIN\(2025\) 977 final](https://data.europa.eu/eli/reg/2025/977/oj)).

met afhankelijkheid, onder meer als gevolg van door derde landen vastgestelde wetgeving met extraterritoriale werking, kunnen worden aangepakt¹¹.

- (6) Er moet een kader worden opgezet om de weerbaarheid en veiligheid van de Unie op het gebied van cloud- en AI-technologieën te vergroten, waarbij het cloud- en AI-ecosysteem van de Unie wordt versterkt door de afhankelijkheid te verminderen, de technologische soevereiniteit te vergroten, investeringen te stimuleren en de capaciteiten, de veiligheid, het aanpassingsvermogen en de weerbaarheid van de cloud- en AI-toeleveringsketen van de Unie te versterken.
- (7) Met het kader worden afzonderlijke doelstellingen nagestreefd en het berust op twee verschillende rechtsgrondslagen.
- (8) Ten eerste is het noodzakelijk om het concurrentievermogen, de capaciteit en de weerbaarheid van de technologische en industriële basis van de Unie op het gebied van cloud en AI te versterken, overeenkomstig artikel 173, lid 3, van het Verdrag betreffende de werking van de Europese Unie (VWEU). Dergelijke maatregelen mogen geen betrekking hebben op de harmonisatie van nationale wet- en regelgeving. Daartoe worden bij deze verordening het initiatief voor cloudleiderschap en het initiatief voor AI-leiderschap (de “initiatieven voor cloud- en AI-leiderschap”) ingesteld om de ontwikkeling van geavanceerde cloud- en AI-technologieën en -faciliteiten te bevorderen en te zorgen voor een brede toepassing daarvan, waarbij de kloof wordt overbrugd tussen de geavanceerde onderzoeks- en innovatiecapaciteiten van de Unie en de duurzame benutting daarvan.
- (9) Ten tweede kunnen de beschikbare computingcapaciteit en de weerbaarheid van het cloud- en AI-ecosysteem het best worden aangepakt door middel van harmonisatiemaatregelen van de Unie op basis van artikel 114 VWEU. Er is één samenhangend regelgevingskader nodig waarin bepaalde voorwaarden voor aanbieders en gebruikers van cloudcomputingdiensten, inclusief capaciteitsopbouw en het aanbieden van cloudcomputingdiensten, worden geharmoniseerd, teneinde de werking van de interne markt te waarborgen.
- (10) De definitie van “cloudcomputingdienst” in deze verordening moet dezelfde zijn als die in artikel 6, punt 30), van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad¹², waarin een “cloudcomputingdienst” wordt gedefinieerd als een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn. Deze definitie van “cloudcomputingdienst” omvat toegang op verzoek tot AI-systemen zoals gedefinieerd in artikel 3, punt 1), van Verordening (EU) 2024/1689 (“verordening artificiële intelligentie”)¹³ van het Europees Parlement en de Raad, die op afstand worden gehost

¹¹ Conclusies van de Raad inzake het Europese concurrentievermogen in het digitale decennium, 5 december 2025 (<https://data.consilium.europa.eu/doc/document/ST-16430-2025-INIT/nl/pdf>).

¹² Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27 december 2022, blz. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

¹³ Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).

en beheerd. Alleen de levering en het ter beschikking stellen van een AI-systeem maken deel uit van de dienst. Het AI-systeem zelf en het daaraan ten grondslag liggende model vallen buiten de reikwijdte van deze definitie.

- (11) De initiatieven voor cloud- en AI-leiderschap moeten het concurrentievermogen en de weerbaarheid van de technologische en industriële basis van de Unie op het gebied van cloud en AI versterken, terwijl tegelijkertijd het innovatievermogen van haar cloud- en AI-ecosysteem wordt versterkt en de uitrol van grootschalige digitale infrastructuur wordt gerealiseerd, in overeenstemming met de doelstellingen die zijn vastgelegd in het actieplan voor het AI-continent en de AI-toepassingsstrategie. Met name de initiatieven voor cloud- en AI-leiderschap moeten de cloud- en datacentrumcapaciteit van de Unie vergroten en tegelijkertijd geavanceerde cloud- en AI-technologieën bevorderen, evenals een brede toepassing van cloud en AI in de gehele economie van de Unie. Zij moeten ook bijdragen aan geavanceerd onderzoek naar de sectorspecifieke toepassing van grensverleggende, fysieke en industriële AI. De AI-toepassingsstrategie moet de ambities en doelstellingen uit het actieplan voor het AI-continent verder uitbouwen en moet waar nodig worden geactualiseerd om rekening te houden met de nieuwste technologische ontwikkelingen en de vooruitgang die is geboekt in het kader van de initiatieven voor cloud- en AI-leiderschap.
- (12) Om de verwezenlijking van die algemene doelstellingen na te streven, moeten de initiatieven voor cloud- en AI-leiderschap aanvullende operationele doelstellingen ondersteunen die zijn uitgewerkt als concrete initiatieven die op Unieniveau moeten worden uitgevoerd.
- (13) Om datacentra in staat te stellen een sleutelrol te spelen bij een duurzame digitale transitie, moeten de initiatieven voor cloud- en AI-leiderschap de onderzoeks- en innovatiecapaciteiten ondersteunen voor de ontwikkeling van datacentrumtechnologieën waarin beginselen van energie- en hulpbronnefficiëntie zowel in het ontwerp als tijdens de exploitatie zijn geïntegreerd, met het oog op het realiseren van duurzaamheid op grote schaal. Dit omvat onder meer het bevorderen van hulpbronnen- en gebruiksefficiënte computingtechnologieën, zoals het optimaliseren van de energie- en waterefficiëntie, het gebruik van opkomende kwantumcomputingtechnologieën, de ontwikkeling van op AI gebaseerde technologieën voor serverefficiëntie, de integratie van computinginfrastructuur met energienetten, en het stimuleren van de invoering van schone energie en energieopwekking ter plaatse in datacentra. De initiatieven voor cloud- en AI-leiderschap moeten ook toegang bieden tot proeflijnen voor datacentrumtechnologieën om de acceptatie van innovaties op de markt te sturen en te versnellen. Dergelijke proefprojecten moeten fungeren als demonstratiefaciliteiten voor ultramoderne halfgeleidertechnologieën voor datacentra en edge-toepassingen, prototypen voor kwantumcomputing en op AI gebaseerde instrumenten voor het beheer van datacentra.
- (14) De initiatieven voor cloud- en AI-leiderschap moeten ook onderzoek, ontwikkelingsactiviteiten en de invoering van cloudstacktechnologieën ondersteunen, met het oog op het dichten van de capaciteitskloof en het versterken van de technologische autonomie van de Unie. De initiatieven voor cloud- en AI-leiderschap moeten met name de ontwikkeling van alternatieven voor cloudcomputingstacks in strategische sectoren stimuleren. Zij moeten tevens de ontwikkeling bevorderen van voor AI geoptimaliseerde servers en software, waaronder in de Unie vervaardigde en ontworpen processoren en accelerators, zoals die welke zijn ontwikkeld in het kader

van Verordening (EU) 2026/XXX¹⁴ van het Europees Parlement en de Raad. Bovendien moeten zowel de initiatieven voor cloud- en AI-leiderschap in het kader van deze verordening als het door die verordening ondersteunde “Chips voor Europa”-initiatief 2.0 het gezamenlijk ontwerpen en de onderlinge optimalisatie van de ontwikkeling van hardware en software, alsmede de integratie van AI-computinginfrastructuur bevorderen. Daarnaast moeten de initiatieven voor cloud- en AI-leiderschap de complementaire ontwikkeling en invoering ondersteunen van een slim en veilig middlewarecloudplatform voor gemeenschappelijke Europese dataruimten, in overeenstemming met de Data Union Strategy.

- (15) De initiatieven voor cloud- en AI-leiderschap moeten tevens de ontwikkeling bevorderen van technologieën die gebaseerd zijn op open normen, open specificaties en opensource, en de ontwikkeling stimuleren van innovatieve, concurrerende en weerbare cloud- en AI-technologieën. Zij moeten de werkzaamheden op het gebied van open normen en specificaties bevorderen, evenals de ontwikkeling van fundamentele opensourcesoftware die het ontwerp, de ontwikkeling en het onderhoud van opensourcecomponenten ondersteunt, met name door te voorzien in governance- en coördinatiemechanismen en door het bundelen van middelen te vergemakkelijken. In het kader van de initiatieven voor cloud- en AI-leiderschap moet ook een catalogus van softwarehulpmiddelen worden opgesteld, waaronder opensourcehulpmiddelen, om koppelingen met bestaande catalogi voor de particuliere en publieke sector mogelijk te maken en om een éénloketsysteem voor opensourcemiddelen in de Unie te ontwikkelen.
- (16) Grensverleggende AI-technologieën maken een snelle ontwikkeling door en zullen naar verwachting een vergaande invloed hebben op de economie en de samenleving van de Unie. Aangezien deze technologieën cruciale strategische activa zijn geworden, is het essentieel dat de Unie haar capaciteit om deze technologieën te ontwikkelen en te reguleren versterkt, om ervoor te zorgen dat de overgang naar artificiële intelligentie in overeenstemming is met de waarden, veiligheidsnormen en economische belangen van de Unie op de lange termijn. Door baanbrekende projecten te ondersteunen, moet de Unie essentiële doorbraken op grotere schaal toepassen om haar concurrentievoordeel in de mondiale digitale economie te behouden. Het stimuleren van de ontwikkeling van grensverleggende AI-technologieën als strategische activa zou ook de huidige afhankelijkheid van technologieën uit derde landen moeten verminderen en het AI-ecosysteem van de Unie moeten versterken.
- (17) De opkomst van fysieke AI, waarmee AI-systemen en -modellen worden bedoeld die de fysieke omgeving kunnen waarnemen en daarbinnen complexe handelingen kunnen uitvoeren, vormt een veelbelovend nieuw terrein waarop geavanceerde digitale intelligentie wordt geïntegreerd in tastbare systemen, zoals robotica, autonome drones en zelfrijdende voertuigen. Fysieke AI is essentieel om externe afhankelijkheid te verminderen en het industriële concurrentievermogen en de strategische autonomie te bevorderen. Dit vereist een doelgerichte aanpak op het gebied van gegevens en computinginfrastructuur. Het is daarom noodzakelijk om het verzamelen en verwerken van hoogwaardige gegevens en de toegang tot computingmiddelen te vergemakkelijken. Bovendien is gerichte ondersteuning nodig voor het testen en valideren van fysieke AI-modellen en -systemen in diverse praktijkomgevingen om de robuustheid en betrouwbaarheid ervan te waarborgen.

¹⁴ Verwijzingen naar de chipsverordening 2.0 worden toegevoegd zodra deze is vastgesteld. Zie het voorstel van de Commissie [verwijzing toevoegen zodra het is gepubliceerd].

- (18) De digitale transformatie van de belangrijkste sectoren van de Unie vormt een centrale pijler van de AI-toepassingsstrategie. Het versnellen van de invoering van AI in die strategische sectoren is essentieel om het mondiale concurrentievermogen te behouden en de maatschappelijke voordelen te vergroten. De initiatieven voor cloud- en AI-leiderschap moeten de ontwikkeling en toepassing van industriële AI in de strategische industriële en dienstensectoren van de Unie versnellen, en tegelijkertijd de technologische ontwikkeling bevorderen van zeer geschikte, sectorspecifieke AI-modellen die zijn ontworpen om te voldoen aan de operationele vereisten van de sectoren die in het kader van de AI-toepassingsstrategie prioriteit hebben gekregen, zoals de gezondheidszorg, het vervoer (inclusief de lucht- en ruimtevaart), de automobielsector, de be- en verwerkende industrie, defensie en ruimtevaart, klimaat en milieu, en de agrovoedingssector. De initiatieven voor cloud- en AI-leiderschap moeten ook de ontwikkeling versnellen van de dienstensectoren die in de AI-toepassingsstrategie als prioritair zijn aangemerkt, evenals wetenschappelijke ontdekkingen als prioriteiten in de Europese strategie voor AI in de wetenschap, in overeenstemming met COM(2025) 724 final.
- (19) In de gezondheidszorg zouden deze ontwikkelingen de nauwkeurigheid van klinische beslissingen moeten verbeteren en de farmaceutische sector ingrijpend moeten veranderen. In de automobielsector moeten zij de ontwikkeling, het testen en de invoering ondersteunen van innovatieve softwareplatformen die bijdragen aan het industriële leiderschap van de Unie op het gebied van softwaregedefinieerde voertuigen en autonoom rijden. De initiatieven voor cloud- en AI-leiderschap moeten ook de belemmeringen voor het testen en in gebruik nemen van AI-modellen verminderen, met name in steden en regio's die bijdragen aan de ontwikkeling van het leiderschap van de Unie op het gebied van softwaregedefinieerde voertuigen en autonoom rijden. Bovendien moeten de lidstaten de ontwikkeling, het testen en de invoering van AI-systemen voor autonoom rijden bevorderen, onder meer door samenwerking met de centra voor AI, de automobielsector, toeleveranciers, steden en regio's, teneinde een veilige en betrouwbare invoering van op AI gebaseerde, verbonden en autonome mobiliteitsoplossingen in uiteenlopende Europese omgevingen mogelijk te maken. In de be- en verwerkende industrie moet de Commissie het bundelen van gegevens tussen verschillende industriële sectoren via betrouwbare derde partijen faciliteren om gespecialiseerde AI-modellen te trainen, waarbij een toereikende hoeveelheid trainingsdata wordt gewaarborgd en de intellectuele-eigendomsrechten strikt worden geëerbiedigd. Er moet onderzoek worden gedaan naar veilige en verifieerbare computingmethoden om het gebruik van AI in gevoelige contexten mogelijk te maken. In de defensiesector, waar AI zich heeft ontpopt als een disruptieve technologie met aanzienlijke gevolgen voor veiligheid en defensie, zouden de initiatieven voor cloud- en AI-leiderschap de ontwikkeling van geavanceerde capaciteiten kunnen ondersteunen, in volledige complementariteit met en zonder afbreuk te doen aan de specifieke instrumenten van de Unie ter ondersteuning van de defensie-industrie, waaronder het Europees Defensiefonds ("EDF") en het programma voor de Europese defensie-industrie ("EDIP"). In de ruimtevaartsector zouden digitale ontwikkelingen de manier waarop ruimtevaartactiva, -diensten en -gegevensstromen worden beheerd en gebruikt, moeten veranderen, en op het gebied van vervoer zouden digitale ontwikkelingen in de luchtvaart de manier waarop de bedrijfsvoering wordt aangestuurd, moeten veranderen, waarbij AI gebruikmaakt van decennia aan beschikbare missie-, operationele en observatiegegevens. Op het gebied van klimaat en milieu moet geospatiale AI worden ontwikkeld, met name door gebruik te maken van aardobservatiegegevens uit het

Copernicus-programma en de mogelijkheden van de ruimtevaart- en connectiviteitsprogramma's van de Unie in het algemeen¹⁵. In de landbouw kan AI gegevens van sensoren, satellieten en landbouwmachines omzetten in bruikbare inzichten voor boeren. AI kan het concurrentievermogen en de weerbaarheid versterken, bijvoorbeeld door opbrengstprognosen te verbeteren, vroegtijdige opsporing van plagen en ziekten mogelijk te maken, de irrigatie en het gebruik van meststoffen te optimaliseren en een duurzamere voedselproductie te ondersteunen. Aangezien de toepassing van AI in industriële contexten een grondige validatie in praktijkomgevingen vereist, moet de Unie industriële actoren voorzien van cloudgebaseerde AI-hulpmiddelen en testomgevingen.

- (20) De Unie moet ook de beschikbaarheid bevorderen van streng beveiligde computinginfrastructuur voor het trainen, testen en in gebruik nemen van defensiegerelateerde AI-modellen en -systemen.
- (21) Naarmate AI-agenten steeds bekwaamer zijn geworden en AI-toepassingen steeds dieper zijn ingebed in praktijksituaties binnen het bedrijfsleven, evolueert de sector in hoog tempo naar een nieuw paradigma waarin dergelijke systemen worden uitgerust met autonome uitvoeringsmogelijkheden. Deze transitie naar een nieuw paradigma vereist een robuust technisch kader om de veiligheid, nauwkeurigheid en wetgevingsnaleving van die systemen te waarborgen, gezien de strenge technische eisen die aan AI-platformen worden gesteld. De initiatieven voor cloud- en AI-leiderschap moeten dan ook gericht zijn op het opzetten van soevereine en veilige AI-platformen die bestemd zijn voor de grootschalige inzet en coördinatie van geavanceerde AI-agenten. Die platforms moeten worden ondersteund door innovatieve coördinatiekaders die zorgen voor transparantie en verantwoording bij interacties tussen meerdere actoren. Het is ook noodzakelijk om de ontwikkeling van strenge test- en experimentele methodologieën voor AI-agenten en -coördinatie te bevorderen, teneinde onbedoeld autonoom gedrag tot een minimum te beperken.
- (22) De initiatieven voor cloud- en AI-leiderschap moeten de ontwikkeling en invoering van AI-modellen en -systemen in de hele publieke sector van de Unie stimuleren. AI-modellen en -systemen moeten met name worden ingezet om betere besluitvorming te ondersteunen, administratieve procedures te vereenvoudigen en onnodige lasten te verminderen, met name op cruciale publieke terreinen zoals de gezondheidszorg, waar het hergebruik van gegevens voor AI-modellen en -hulpmiddelen moet worden bevorderd, waarbij de veiligheid en de gegevensbescherming gewaarborgd moeten blijven. Daartoe is het wenselijk maatregelen te nemen om de kwaliteit van overheidsgegevens te verbeteren en het delen en hergebruiken van trainingsdata en AI-modellen binnen de publieke sector van de Unie te bevorderen, waardoor versnippering wordt voorkomen en succesvolle, gebruikersgerichte oplossingen kunnen worden opgeschaald.
- (23) De initiatieven voor cloud- en AI-leiderschap moeten helpen om de invoering van AI en cloudcomputing op grote schaal te versnellen, ook op regionaal en lokaal niveau. De brede toepassing van AI in de particuliere en de publieke sector moet worden bevorderd via het netwerk van centra voor AI. Door gebruik te maken van dit netwerk, moeten aanvullende ondersteunende maatregelen worden ontwikkeld om de

¹⁵ Verordening (EU) 2021/696 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van het ruimtevaartprogramma van de Unie, tot oprichting van het Agentschap van de Europese Unie voor het ruimtevaartprogramma en tot intrekking van de Verordeningen (EU) nr. 912/2010, (EU) nr. 1285/2013 en (EU) nr. 377/2014 en Besluit nr. 541/2014/EU (PB L 170 van 12.5.2021, blz. 69, ELI: <http://data.europa.eu/eli/reg/2021/696/oj>).

doelstelling van de digitale transformatie van bedrijven te helpen verwezenlijken, zoals vastgelegd in Besluit (EU) 2022/2481 van het Europees Parlement en de Raad¹⁶ (“het beleidsprogramma voor het digitale decennium tot 2030”). Bovendien moet er een specifiek leerplan voor vaardigheden op het gebied van cloudcomputing en AI worden ontwikkeld om werknemers in zowel de publieke als de particuliere sector te voorzien van geavanceerde competenties, teneinde de afhankelijkheid van aanbieders van buiten de EU te verminderen en capaciteiten van de volgende generatie te ontwikkelen, in overeenstemming met het beleid van de Unie op het gebied van onderwijs, opleiding en vaardigheden, waaronder de mededeling over de vaardigheidsunie¹⁷. Waar relevant moet het leerplan voortbouwen op desbetreffende Europese initiatieven, waaronder de academie voor AI-vaardigheden, de centra voor AI en de academie voor een interoperabel Europa, en moet het de deelname omvatten van belanghebbenden met de nodige expertise.

- (24) De initiatieven voor cloud- en AI-leiderschap moeten er ook voor zorgen dat cloudcomputingdiensten van Europese aanbieders in zowel de publieke als de particuliere sector op grotere schaal worden ingezet, zodat de invoering van cloudcomputing in overeenstemming is met de doelstelling om de technologische autonomie van de Unie te versterken, met name in sectoren zoals de gezondheidszorg en het onderwijs, waar kritieke gegevens worden verwerkt. Bij de verwezenlijking van deze doelstelling zou gebruik kunnen worden gemaakt van de resultaten van de relevante Europese consortia voor digitale infrastructuur (“EDIC’s”), waaronder gedeelde infrastructuur, gemeenschappelijke normen en beste praktijken. De initiatieven voor cloud- en AI-leiderschap moeten de oprichting van de Europese cloudfederatie voor de publieke sector (“Federatie EuroCloud”) in het kader van deze verordening ondersteunen, teneinde het delen van veilige en weerbare datacentrumdiensten en cloudcomputingdiensten voor de publieke sector te vergemakkelijken. Bovendien moeten de initiatieven voor cloud- en AI-leiderschap de aanbestedingsactiviteiten ondersteunen die de Commissie uitvoert ten behoeve van instellingen, organen en instanties van de Unie (“entiteiten van de Unie”), maar ook ten behoeve van nationale aanbestedende diensten in de hele Unie, aangezien de aanbesteding van digitale diensten niet alleen de digitalisering van overheidsinstanties moet bevorderen, maar hen ook in staat moet stellen hun koopkracht te benutten en de invoering van weerbare en veilige digitale oplossingen te versnellen.
- (25) De lidstaten zouden ervarings- en versnellingscentra voor AI (“centra voor AI”) op moeten richten om te zorgen voor een passende dekking van hun grondgebied. Centra voor AI moeten fungeren als regionale en lokale versnellers voor de invoering en toepassing van AI, cloudcomputing en andere geavanceerde technologieën in de hele Unie, en zo kmo’s, kleine midcaps en openbare lichamen ondersteunen bij hun digitale transformatie. Om de integratie van AI in strategische industriële sectoren te vergemakkelijken, moeten centra voor AI ook synergieën tot stand brengen met initiatieven die in het kader van de Data Union Strategy zijn gelanceerd. Door expertise, testmogelijkheden, vaardigheden en ondersteuning op het gebied van innovatie te bieden, moeten centra voor AI het concurrentievermogen en de weerbaarheid van de industriële basis van de Unie op het gebied van AI versterken en

¹⁶ Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030 (PB L 323 van 19.12.2022, blz. 4, ELI: <http://data.europa.eu/eli/dec/2022/2481/oj>).

¹⁷ Mededeling van de Commissie aan het Europees Parlement, de Europese Raad, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio’s van 5 maart 2025, “De vaardigheidsunie” (COM(2025) 90 final).

tegelijkertijd de innovatiecapaciteit en de brede toepassing van AI en andere geavanceerde technologieën in de hele Unie bevorderen. Het netwerk moet voortbouwen op het netwerk van Europese digitale-innovatiehubs. Het netwerk zal nauw samenwerken met andere initiatieven die de invoering van AI en andere geavanceerde technologieën ondersteunen, zoals voorzieningen voor het testen van en experimenteren met AI en AI-fabrieken. Het zal voortbouwen op initiatieven op het gebied van vaardigheden, waaronder het grootschalige digitale partnerschap van het pact voor vaardigheden en de academies voor vaardigheden, waaronder de academie voor AI-vaardigheden.

- (26) De uitvoering van de initiatieven voor cloud- en AI-leiderschap moet worden toevertrouwd aan de Commissie en de lidstaten. De uitvoering van de initiatieven voor cloud- en AI-leiderschap moet, indien van toepassing, ook worden toevertrouwd aan andere instanties die over de nodige expertise en middelen beschikken. In het bijzonder moet het, onverminderd het volgende meerjarig financieel kader (2028-2034), mogelijk zijn om de uitvoering van de initiatieven voor cloud- en AI-leiderschap toe te vertrouwen aan gemeenschappelijke ondernemingen, zoals de Gemeenschappelijke Onderneming “Slimme netwerken en diensten” (“de GO”), opgericht bij Verordening (EU) 2021/2085 van de Raad¹⁸ of de Gemeenschappelijke Onderneming Europese high-performance computing (“de GO EuroHPC”), opgericht bij Verordening (EU) 2021/1173 van de Raad¹⁹ en, indien van toepassing, de opvolgers daarvan.
- (27) De operationele doelstellingen van de initiatieven voor cloud- en AI-leiderschap moeten met name worden gerealiseerd door ambitieuze, toekomstgerichte doelstellingen vast te stellen die erop gericht zijn verder te gaan dan de huidige stand van de techniek op het gebied van infrastructuurontwikkeling, cloudcomputing en AI. De initiatieven voor cloud- en AI-leiderschap moeten daarom strategische “grote uitdagingen” ondersteunen die gericht zijn op de ontwikkeling en toepassing van geavanceerde cloud- en AI-technologieën en -infrastructuur die cruciaal zijn voor de Unie. Die grote uitdagingen moeten voortbouwen op de uitdagingen die zijn vastgelegd in Verordening (EU) 2026/XXX [chipsverordening 2.0] betreffende een kader voor maatregelen ter versterking van het halfgeleiderecosysteem van de Unie, dat tot doel heeft halfgeleider technologieën mogelijk te maken die ten grondslag liggen aan AI-, cloudcomputing-, datacentrum- en edge-infrastructuur.
- (28) De initiatieven voor cloud- en AI-leiderschap kunnen worden ondersteund met middelen uit programma’s en andere instrumenten van de Unie, met name uit Horizon Europa en het programma Digitaal Europa, alsook uit het InvestEU-programma, overeenkomstig Verordening (EU) 2021/694²⁰, Verordening (EU) 2021/695²¹ en

¹⁸ Verordening (EU) 2021/2085 van de Raad van 19 november 2021 voor de oprichting van Gemeenschappelijke Ondernemingen in het kader van Horizon Europa en tot intrekking van Verordeningen (EG) nr. 219/2007, (EU) nr. 557/2014, (EU) nr. 558/2014, (EU) nr. 559/2014, (EU) nr. 560/2014, (EU) nr. 561/2014 en (EU) nr. 642/2014 (PB L 427 van 30.11.2021, blz. 17, ELI: <http://data.europa.eu/eli/reg/2021/2085/oj>).

¹⁹ Verordening (EU) 2021/1173 van de Raad van 13 juli 2021 tot oprichting van de Gemeenschappelijke Onderneming Europese high-performance computing en tot intrekking van Verordening (EU) 2018/1488 (PB L 256 van 19.7.2021, blz. 3, ELI: <http://data.europa.eu/eli/reg/2021/1173/oj>).

²⁰ Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PB L 166 van 11.5.2021, blz. 1, ELI: <http://data.europa.eu/eli/reg/2021/694/oj>).

²¹ Verordening (EU) 2021/695 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van Horizon Europa — het kaderprogramma voor onderzoek en innovatie, tot vaststelling van de regels

Verordening (EU) 2021/523²². In het kader van het meerjarig financieel kader 2028-2034 zouden de initiatieven voor cloud- en AI-leiderschap steun kunnen blijven ontvangen in het kader van opvolgende programma's van de Unie, mits deze worden vastgesteld en in overeenstemming met hun respectieve rechtsgrondslagen.

- (29) Naast financiering in het kader van programma's van de Unie kunnen de initiatieven voor cloud- en AI-leiderschap door de lidstaten worden ondersteund via maatregelen op het gebied van onderzoek, ontwikkeling en innovatie, in overeenstemming met de geldende regels inzake staatssteun, waarbij ervoor wordt gezorgd dat het nationale beleid en het beleid van de Unie onderling samenhangend zijn, alsook via investeringen uit de particuliere sector. Belanghebbenden uit de particuliere sector moeten met name worden aangemoedigd om bij het uitstippelen van hun investeringsstrategieën voor cloudcomputing en AI rekening te houden met de initiatieven voor cloud- en AI-leiderschap. Op die manier kunnen particuliere investeringen bijdragen aan een samenhangend en gecoördineerd investeringstraject dat aansluit bij de bredere beleidsdoelstellingen en de langetermijndoelen voor de uitvoering die zijn vastgelegd in de initiatieven voor cloud- en AI-leiderschap.
- (30) De Commissie moet advies vragen van belanghebbenden met de nodige expertise over de uitvoering van de initiatieven voor cloud- en AI-leiderschap. De Commissie moet met name de samenwerking bevorderen met bestaande deskundigen- en adviesfora, zoals de alliantie voor industriële gegevens, edge en cloud, de AI-toepassingsalliantie en de industriële alliantie voor halfgeleiders. De alliantie voor industriële gegevens, edge en cloud moet fungeren als een forum voor uitwisseling tussen diverse belanghebbenden op het gebied van edge- en cloudtechnologieën van de volgende generatie, waaronder bedrijven, vertegenwoordigers van de lidstaten en andere relevante deskundigen. Dit zou de Commissie moeten helpen bij het opstellen van strategische investeringsroutekaarten om de volgende generatie uiterst veilige, gedistribueerde, interoperabele en hulpbronnefficiënte computingtechnologieën mogelijk te maken. De AI-toepassingsalliantie moet fungeren als coördinatieforum voor belanghebbenden en beleidsmakers op het gebied van AI, om de discussie over het potentieel van AI in strategische sectoren van de Unie te bevorderen. De AI-toepassingsalliantie moet blijven bijdragen aan de verwezenlijking van de doelstellingen van de AI-toepassingsstrategie, met name door workshops voor het bedrijfsleven te organiseren, nieuwe toepassingen van AI in strategische sectoren in kaart te brengen en te beoordelen en voor specifieke ondersteunende beleidsmaatregelen te pleiten. Naast de AI-toepassingsalliantie moet het AI-waarnemingscentrum betrouwbare indicatoren aanreiken om de impact van AI op strategische sectoren te beoordelen en technologische ontwikkelingen en trends te monitoren, evenals de veranderingen die dit op de arbeidsmarkt teweeg kan brengen.
- (31) De initiatieven voor cloud- en AI-leiderschap moeten de synergieën versterken met maatregelen die momenteel door de Unie en de lidstaten worden ondersteund, onder meer in het kader van Horizon Europa en het programma Digitaal Europa, alsook Verordening (EU) 2021/1173 van de Raad en Verordening (EU) 2026/XXX [chipsverordening 2.0] betreffende een kader voor maatregelen ter versterking van het halfgeleiderecosysteem van de Unie. De Commissie en de lidstaten moeten zorgen

²² voor deelname en verspreiding en tot intrekking van Verordeningen (EU) nr. 1290/2013 en (EU) nr. 1291/2013 (PB L 170 van 12.5.2021, blz. 1, ELI: <http://data.europa.eu/eli/reg/2021/695/oj>). Verordening (EU) 2021/523 van het Europees Parlement en de Raad van 24 maart 2021 tot vaststelling van het InvestEU-programma en tot wijziging van Verordening (EU) 2015/1017 (PB L 107 van 26.3.2021, blz. 30, ELI: <http://data.europa.eu/eli/reg/2021/523/oj>).

voor samenhang, complementariteit en synergieën tussen de initiatieven voor cloud- en AI-leiderschap, en toepasselijke nationale en regionale strategieën, programma's en investeringsplannen, inclusief die welke worden uitgevoerd in het kader van nationale hervormingsprogramma's, strategieën voor slimme specialisatie, herstel- en veerkrachtplannen en andere nationale of regionale financieringsinstrumenten die de doelstellingen van de initiatieven voor cloud- en AI-leiderschap ondersteunen. Een dergelijke coördinatie moet erop gericht zijn het effect van overheidsinvesteringsen te maximaliseren, dubbele financiering te voorkomen, de afstemming van prioriteiten tussen de verschillende bestuursniveaus te bevorderen en de opschaling en toepassing van resultaten in de hele Unie te vergemakkelijken.

- (32) Om ervoor te zorgen dat het beleid van de Unie en dat van de lidstaten onderling samenhangend is, moeten de lidstaten nationale strategieën vaststellen die bijdragen aan de verwezenlijking van de doelstellingen van de Unie op het gebied van de ontwikkeling van cloudtechnologie en AI, in overeenstemming met het actieplan voor het AI-continent en de AI-toepassingsstrategie. De nationale strategieën moeten met name het AI-eerst-beginsel bevatten dat in de AI-toepassingsstrategie is vastgelegd, waarbij organisaties worden aangespoord om na te denken over hun bedrijfsprocessen, rekening houdend met de behoeften en kansen die AI biedt, en tegelijkertijd oog te hebben voor de mogelijke risico's. De nationale cloud- en AI-strategieën moeten ook worden afgestemd op de bijbehorende digitale doelstellingen die zijn vastgesteld in Besluit (EU) 2022/2481²³, met name wat betreft de invoering van cloudcomputingdiensten, big data en AI door ten minste 75 % van de ondernemingen in de Unie voor hun bedrijfsactiviteiten, en de inzet van ten minste 10 000 klimaatneutrale, zeer goed beveiligde edge nodes in de Unie, waarbij een lage latentie wordt gewaarborgd. De maatregelen die in het kader van de nationale strategieën zijn genomen, zouden als uitgangspunt kunnen dienen voor de nationale strategische stappenplannen voor het digitale decennium ("de nationale stappenplannen").
- (33) Indien een lidstaat al een nationale strategie heeft vastgesteld die de in deze verordening vastgestelde doelstellingen op adequate wijze bestrijkt, mag van die lidstaat niet worden verlangd dat hij een andere strategie vaststelt. Mocht een lidstaat echter in het licht van die doelstellingen tekortkomingen in zijn bestaande strategie vaststellen, dan moet hij deze dienovereenkomstig aanpassen. De Europese raad voor artificiële intelligentie, opgericht bij de verordening artificiële intelligentie ("de AI-board"), speelt een centrale rol bij het waarborgen van een consistente en doeltreffende uitvoering van het Uniebeleid inzake artificiële intelligentie. Aangezien cloudcomputing de basis vormt voor en de drijvende kracht is achter AI, moet de AI-board fungeren als platform om de samenwerking en coördinatie tussen de Unie en de lidstaten te bevorderen bij activiteiten die verband houden met de invoering van AI. Om deze taak te kunnen uitvoeren, moet de AI-board beschikken over de nodige expertise en een passende samenstelling hebben.
- (34) Gezien de ongekennde omvang van de middelen die nodig zijn voor de ontwikkeling van grensverleggende AI, is het noodzakelijk criteria vast te stellen voor de aanwijzing van een project als prioritair project op het gebied van grensverleggende AI. Dergelijke projecten moeten de ontwikkeling en opschaling van grensverleggende AI-technologieën ondersteunen, met name op het gebied van cyberbeveiliging. Gezien hun technische complexiteit en het feit dat het om kapitaalintensieve projecten gaat,

²³ Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030 (PB L 323 van 19.12.2022, blz. 4, ELI: <http://data.europa.eu/eli/dec/2022/2481/oj>).

vereisen deze projecten een gezamenlijke aanpak op het niveau van de Unie. Het is derhalve passend om bij deze projecten als vereiste te stellen dat er wordt gezorgd voor een brede deelname van entiteiten uit de hele Unie, met name via EDIC's die zijn opgericht krachtens Besluit (EU) 2022/2481 of via enige andere juridische structuur die een aanzienlijk deel van de belangen van de Unie kan vertegenwoordigen.

- (35) De toewijzing van voldoende AI-computingmiddelen aan prioritaire projecten op het gebied van grensverleggende AI moet van strategisch belang zijn voor de Unie en de lidstaten. De Unie moet, op evenredige basis en binnen de grenzen van de beschikbare capaciteit op het gebied van Europese high-performance computing ("EuroHPC"), een bijdrage leveren die gelijk is aan de AI-computingmiddelen die de lidstaten hebben bijgedragen of toegezegd voor de aangewezen prioritaire projecten op het gebied van grensverleggende AI. De Unie en de lidstaten moeten ook voldoende computingtijd ter beschikking stellen voor industriële innovatie op het gebied van AI, fysieke AI en AI-projecten in de publieke sector. Dit laat de voorschriften en procedures van Verordening (EU) 2021/1173 van de Raad onverlet. Het toegangsbeleid van de GO EuroHPC moet zodanig worden aangepast dat de toewijzing van dergelijke computingmiddelen op een efficiënte, transparante en tijdige wijze plaatsvindt, zonder afbreuk te doen aan de continuïteit van de lopende activiteiten en de rechten van projecten die reeds gebruikmaken van toegewezen EuroHPC-computingmiddelen voor AI.
- (36) Om de ambities van de Unie op het gebied van artificiële intelligentie te verwezenlijken, is het noodzakelijk om de digitale infrastructuur te versterken en daarin te investeren, waaronder cloud- en edgecapaciteit die het mogelijk maakt om modellen te trainen, te verfijnen, in gebruik te nemen en in realtime te laten draaien. De uitrol van datacentra in de Unie verloopt traag en blijft geconcentreerd in een beperkt aantal gevestigde hubs, wat leidt tot structurele onevenwichtigheden tussen de lidstaten en tot inefficiënties zoals hogere kosten, grotere latentie voor perifere regio's, ongelijke kansen voor bedrijven en een tragere digitale transformatie. Het uitbreiden en geografisch evenwichtig verdelen van de capaciteit van datacentra in de hele Unie is eveneens cruciaal om de afhankelijkheid van externe infrastructuur te verminderen, waardoor economische veiligheidsrisico's worden beperkt en het concurrentievermogen, de weerbaarheid en de soevereiniteit van de Unie worden ondersteund.
- (37) Datacentra vormen een cruciale infrastructuur voor de Unie en kunnen aanzienlijke economische waarde genereren, waaronder waardevolle investeringen en banen, en kunnen innovatie-ecosystemen ondersteunen, vooral als ze zijn afgestemd op de lokale behoeften en de beste praktijken volgen. Als dit op de juiste wijze wordt beheerd, kan de uitbreiding van de capaciteit van datacentra in de Unie aanzienlijke economische en strategische voordelen opleveren, bijdragen aan de modernisering van het energiesysteem en de groei van schone energie en het duurzame gebruik van energie ondersteunen. Dit hangt af van de invoering van een adequaat kader dat negatieve gevolgen, zoals druk op de energievoorziening, schadelijke milieueffecten en gemiste kansen, voorkomt. Zones voor de versnelde uitrol van datacentra ("versnellingszones") moeten aan deze doelstelling bijdragen door de uitrol van infrastructuur op grote schaal en in hoog tempo mogelijk te maken binnen een duidelijk en gestroomlijnd regelgevingskader.
- (38) Wanneer er op het grondgebied van de lidstaten capaciteit wordt ingezet, moeten er versnellingszones worden aangewezen waar de ontwikkeling, uitbreiding en modernisering van datacentra kunnen worden bevorderd. De aanwijzing van dergelijke

zones moet bijdragen aan het wegwerken van de capaciteitstekorten in de Unie en het concurrentievermogen, de autonomie en de technologische weerbaarheid van de Unie vergroten, waarbij tegelijkertijd wordt gezorgd voor naleving van het toepasselijke Unierecht, inclusief de voorschriften inzake energie-efficiëntie en milieubescherming. Een toereikende en tijdige energievoorziening aan de versnellingszones is een fundamentele randvoorwaarde voor de doeltreffende uitrol ervan en voor de ontwikkeling van datacentrumcapaciteit in de gehele Unie. Betrouwbare en nauwkeurige informatie over de toekomstige vraag naar energie draagt bij tot een kosteneffectieve ontwikkeling van het net. De lidstaten moeten daarom voor elke versnellingszone een analyse opstellen waarin de huidige en toekomstige energiebehoeften in kaart worden gebracht. Een dergelijke analyse moet tot doel hebben informatie te verstrekken voor de nationale netplanning en zo bij te dragen tot doelgerichte anticiperende investeringen in het net en snellere energieverbindingen voor de versnellingszone. Bij het bepalen van het toepassingsgebied moeten de lidstaten rekening houden met de beschikbaarheid van relevante vervoers- en netwerkinfrastructuur. De resultaten van deze beoordelingen moeten worden weerspiegeld in de nationale netontwikkelingsplannen om toekomstige punten van de energievraag adequaat mee te nemen in de komende netplanning. Om ervoor te zorgen dat in versnellingszones de juiste voorwaarden aanwezig zijn voor de inzet van capaciteit, moeten de lidstaten zorgen voor duidelijke en efficiënte procedures voor netaansluiting en flexibele aansluitingsovereenkomsten, en moeten zij voor exploitanten van datacentra de voorwaarden voor netaansluiting overeenkomstig Richtlijn (EU) 2019/944 verduidelijken. Een aanstaand wetsvoorstel om de elektriciteitsrekeningen in de EU toekomstbestendig te maken, zal stimulansen bieden om op optimale en kostenefficiënte wijze gebruik te maken van de netinfrastructuur en zal systeemvriendelijk verbruik aanmoedigen. Stroomafnameovereenkomsten (“PPA’s”) zijn belangrijke instrumenten voor datacentra, omdat ze zorgen voor prijsstabiliteit op de lange termijn en exploitanten van datacentra tegelijkertijd in staat stellen om op grote schaal schone elektriciteit in te kopen, waardoor een betrouwbare bedrijfsvoering en de transitie naar een schoon energiesysteem worden ondersteund. De lidstaten dienen derhalve het gebruik van PPA’s te bevorderen, ook in versnellingszones, door ongerechtvaardigde belemmeringen en onevenredige of discriminerende procedures of heffingen weg te nemen, teneinde prijsvoorspelbaarheid te bieden.

- (39) Bij het vaststellen van duurzaamheidseisen voor datacentra die in gebruik worden genomen in zones voor de versnelde uitrol van datacentra, moeten de lidstaten ervoor zorgen dat de belangrijkste prestatie-indicatoren, zoals gedefinieerd in Gedelegeerde Verordening (EU) 2024/1364 van de Commissie²⁴ in overeenstemming met Richtlijn (EU) 2023/1791 van het Europees Parlement en de Raad²⁵ worden gebruikt. Het doel is om in de versnellingszones te zorgen voor consistente milieunormen, de energie-efficiëntie te verhogen en de bredere klimaat-, milieu- en duurzaamheidsdoelstellingen van de Unie te ondersteunen. Om bovendien speculatieve reservering van middelen in versnellingszones te voorkomen en te zorgen voor eerlijke, redelijke en niet-discriminerende toegang die daadwerkelijke concurrentie in stand houdt en de tijdige

²⁴ Gedelegeerde Verordening (EU) 2024/1364 van de Commissie van 14 maart 2024 betreffende de eerste fase van de vaststelling van een gemeenschappelijke beoordelingsregeling van de Unie voor datacentra (PB L, 2024/1364, 17.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1364/oj).

²⁵ Richtlijn (EU) 2023/1791 van het Europees Parlement en de Raad van 13 september 2023 betreffende energie-efficiëntie en tot wijziging van Verordening (EU) 2023/955 (herschikking) (PB L 231 van 20.9.2023, blz. 1, ELI: <http://data.europa.eu/eli/dir/2023/1791/oj>).

en efficiënte ontwikkeling van versnellingszones ondersteunt, moeten de lidstaten ervoor zorgen dat de toewijzing en het gebruik van middelen binnen die zones plaatsvinden onder eerlijke, redelijke en niet-discriminerende voorwaarden en geen aanleiding geven tot speculatieve reservering of afschermingspraktijken die de daadwerkelijke concurrentie of de doeltreffende ontwikkeling of het doeltreffende gebruik van die zones kunnen belemmeren.

- (40) Om de ingebruikname van datacentrumprojecten in versnellingszones te vergemakkelijken en te versnellen, moeten de lidstaten centrale informatiepunten aanwijzen of, waar mogelijk, de informatiepunten die zijn aangewezen krachtens Verordening (EU) 2024/1309 van het Europees Parlement en de Raad²⁶ verbeteren of hiermee integreren.
- (41) Bij Verordening (EU) 202X/XXX [inzake het versnellen van milieubeoordelingen]²⁷ is een gemeenschappelijk versnellingskader voor milieubeoordelingen vastgesteld om de uitrol van belangrijke technologieën door de Unie te stimuleren, afhankelijkheden te verminderen en het concurrentievermogen te vergroten. De procedures in verband met milieubeoordelingen moeten worden versneld en gestroomlijnd voor plannen, programma's en projecten in alle sectoren van de economie, met behoud van een hoog beschermingsniveau voor de menselijke gezondheid en het milieu. Voor sommige sectoren zijn echter mogelijk snellere milieubeoordelingen nodig. Om de samenhang van het rechtskader voor milieubeoordelingen te waarborgen en tegelijkertijd tegemoet te komen aan de behoefte aan een versnelde invoering in bepaalde strategische sectoren, wordt bij Verordening (EU) 202X/XXX [inzake het versnellen van milieubeoordelingen] een specifieke toolbox ingesteld. Gezien hun rol bij het waarborgen van de verwezenlijking van de klimaat- en milieudoelstellingen van de Unie door hun bijdrage aan het verbeteren van de energie-efficiëntie, het mogelijk maken van de integratie van schone energie en het verschaffen van de infrastructuur die nodig is voor slimmere netten, vervoerssystemen en koolstofarme technologieën, en gezien hun bijdrage aan de weerbaarheid en economische veiligheid van de Unie door te zorgen voor betrouwbare infrastructuur in de Unie ter bescherming van kritieke diensten en door het versterken van het vermogen van de Unie om onafhankelijk te functioneren, moeten datacentrumprojecten die in versnellingszones worden uitgevoerd, worden beschouwd als strategische projecten in de zin van Verordening (EU) 202X/XXX [inzake het versnellen van milieubeoordelingen] en derhalve gebruik kunnen maken van de specifieke toolbox die krachtens die verordening is vastgesteld. De lidstaten moeten een geaggregeerde basisvergunning vaststellen die recht doet aan de specifieke kenmerken van elke geïdentificeerde versnellingszone. Die door de overheidsinstanties afgegeven geaggregeerde basisvergunning moet de vergunningen omvatten die doorgaans voor dergelijke activiteiten binnen het gebied vereist zijn, met uitzondering van de vergunningen voor aansluiting op het elektriciteitsnet.
- (42) De Commissie moet de mogelijkheid hebben om datacentrumprojecten die een aanzienlijke bijdrage leveren aan de digitale en de energiesector van de Unie en die

²⁶ Verordening (EU) 2024/1309 van het Europees Parlement en de Raad van 29 april 2024 inzake maatregelen om de kosten van de uitrol van elektronische communicatienetwerken met gigabitsnelheden te verlagen, tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Richtlijn 2014/61/EU (gigabitinfrastructuurverordening) (PB L, 2024/1309, 8.5.2024, ELI: <http://data.europa.eu/eli/reg/2024/1309/oj>).

²⁷ Verwijzing toevoegen naar de verordening inzake het versnellen van milieubeoordelingen zodra deze is vastgesteld. Zie het voorstel van de Commissie (COM(2025) 984 final, <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:52025PC0984>).

aan duidelijke criteria voldoen, aan te merken als strategische projecten. Gezien het belang van de strategische datacentrumprojecten kunnen de lidstaten, onverminderd de artikelen 107 en 108 VWEU, op evenredige wijze steunmaatregelen ten behoeve van die projecten toepassen. Bij het plannen van dergelijke steunmaatregelen meten de lidstaten, indien van toepassing, gebruikmaken van de relevante kaders voor het verlenen van overheidssteun. Strategische projecten moeten op evenredige wijze een marktfalen aanpakken, zonder dat dit leidt tot dubbele financiering of verdringing van particuliere financiering, en tegelijkertijd een duidelijke meerwaarde van de Unie opleveren.

- (43) Strategische datacentrumprojecten moeten steun ontvangen uit programma's, fondsen en financiële instrumenten van de Unie, in overeenstemming met de doelstellingen die zijn vastgelegd in de verordening tot instelling van die fondsen en programma's, en onverminderd het volgende meerjarig financieel kader (2028-2034). In het bijzonder moeten aan die strategische projecten het keurmerk worden toegekend voor projecten die bijdragen aan het concurrentievermogen ("concurrentiekeurmerk") indien ze voldoen aan de voorwaarden uit Verordening (EU) 2026/XXX [tot instelling van het Europees Fonds voor concurrentievermogen] (EFC)²⁸, als hoogwaardige projecten die bijdragen aan de doelstelling van het Europees Fonds voor concurrentievermogen.
- (44) Om de strategische inzet van datacentrumcapaciteit in de hele Unie te bevorderen, moet de Commissie de beschikbare computingcapaciteit en de omvang van de vraag naar datacentrumcapaciteit monitoren en de omvang van de capaciteitskloof in de hele Unie in kaart brengen. De Commissie kan deze monitoring gebruiken als basis voor eventuele aanbevelingen. Om de lidstaten te begeleiden bij het versnellen van de uitrol van datacentrumcapaciteit, kan de Commissie, waar nodig, maatregelen aanbevelen om de vastgestelde capaciteitstekorten in de Unie aan te pakken. In overeenstemming met het beleidsprogramma voor het digitale decennium tot 2030 moet de Commissie ook de doelstellingen van het digitale decennium herzien om recht te doen aan de technische, economische of maatschappelijke ontwikkelingen en aan de veranderingen in de prioriteiten van de Unie op dat gebied.
- (45) Deze verordening is van toepassing op de instellingen, organen en instanties van de Unie ("entiteiten van de Unie") bij het uitvoeren van procedures voor de aanbesteding van cloudcomputingdiensten en AI-systemen die binnen het toepassingsgebied van deze verordening vallen.
- (46) De Unie blijft nog steeds in kritieke mate afhankelijk van een beperkt aantal aanbieders van cloudcomputingdiensten die onder de zeggenschap staan van derde landen of in derde landen gevestigde rechtspersonen. Dit stelt de Unie bloot aan kritieke strategische afhankelijkheden en concentratierisico's, waaronder kwetsbaarheden die voortvloeien uit de extraterritoriale toepassing van wetgeving van derde landen, mogelijke verstoringen die de continuïteit, kwaliteit en weerbaarheid van cloudcomputingdiensten aantasten, verminderde zeggenschap over en toezicht op persoonsgegevens en niet-persoonsgegevens en infrastructuur, en het risico dat er ongepaste economische of politieke invloed wordt uitgeoefend via de zeggenschap door derde landen of in derde landen gevestigde rechtspersonen over cloudcomputingdiensten. Tegen deze achtergrond is het voor de Unie en haar lidstaten cruciaal geworden om de zeggenschap te behouden over infrastructuur, gegevens,

²⁸ Verwijzing toevoegen naar de verordening tot instelling van het Europees Fonds voor concurrentievermogen zodra deze is vastgesteld. Zie het voorstel van de Commissie (COM(2025) 555 final/2, <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:52025PC0555R%2801%29>).

activa en technologiesystemen die onder de rechtsbevoegdheid van de Unie en de lidstaten vallen.

- (47) De bestaande Uniewetgeving regelt de vereisten op het gebied van cyberbeveiliging, gegevensbescherming, interoperabiliteit en gegevensoverdraagbaarheid waaraan cloudcomputingdiensten moeten voldoen. Er bestaat echter geen overkoepelend regelgevingskader van de Unie waarin een geharmoniseerde definitie wordt vastgelegd van wat een betrouwbare cloudcomputingdienst is om dergelijke risico's te beperken. Sommige lidstaten hebben nationale benaderingen ontwikkeld, of zijn daarmee bezig, om nationale soevereine diensten in kaart te brengen. Nationale maatregelen bieden echter geen afdoende oplossing voor de landsgrensoverschrijdende vraagstukken die verband houden met het gebrek aan soevereiniteit van de Unie in het cloudcomputingecosysteem, en brengen het risico met zich mee dat de interne markt van de Unie versnipperd raakt en dat de gemeenschappelijke doelstellingen op het gebied van autonomie en soevereiniteit worden ondermijnd.
- (48) Aanbieders van cloudcomputingdiensten hebben op maat gemaakte versies van hun dienstenaanbod gelanceerd als reactie op de toenemende bezorgdheid van de Unie over soevereiniteit. In die versies wordt echter geen aandacht besteed aan de belangrijkste kwesties op het gebied van soevereiniteit, waardoor de wetgeving van derde landen extraterritoriale werking kan hebben en de dienst mogelijk wordt aangetast of verstoord. Bijgevolg waarborgt de Unie geen autonomie of zeggenschap over haar gegevens, activa en digitale infrastructuur. Het huidige kader moet daarom worden aangevuld met gerichte maatregelen op Unieniveau door de invoering van een geharmoniseerd mechanisme dat de langetermijnstrategie van de Unie voor technologische autonomie, zeggenschap en weerbaarheid in het cloud- en AI-ecosysteem kan versterken.
- (49) Tegen deze achtergrond vereist de aanzienlijke toename van de bezorgdheid op het gebied van de openbare orde, waaronder bijvoorbeeld risico's voor de economische veiligheid, een doeltreffende en samenhangende toepassing van waarborgen voor activiteiten die uit de begroting van de Unie worden gefinancierd. Wat de entiteiten van de Unie betreft, worden in artikel 136 van Verordening (EU, Euratom) 2024/2509²⁹ het toepassingsgebied, de regels en de procedures voor het vaststellen en uitvoeren van gevoelige openbare aanbestedingsprocedures vastgelegd.
- (50) Ter bescherming van de openbare orde is het derhalve noodzakelijk om de voorwaarden vast te stellen die de aanbestedende diensten van de Unie en de lidstaten moeten hanteren bij openbare aanbestedingsprocedures voor cloudcomputingdiensten. Bij het kiezen van passende risicobeperkende maatregelen ter handhaving van de openbare orde in de Unie en de lidstaten is het van fundamenteel belang rekening te houden met mogelijke blootstelling aan risico's. Het feit dat de Unie en de lidstaten in hoge mate afhankelijk zijn van een beperkt aantal aanbieders van cloudcomputingdiensten die onder de zeggenschap staan van een derde land of een in een derde land gevestigde rechtspersoon, kan leiden tot risico's zoals misbruik (bv. manipulatie, toegang en controle op afstand, sabotage, gebruik als wapen), toegang tot informatie (bv. toegang tot gevoelige informatie, ongeoorloofde communicatie, het lekken van technologie, gegevensmanipulatie of -exfiltratie, spionage) en kwetsbaarheden als gevolg van afhankelijkheid (bv. politieke en/of economische

²⁹ Verordening (EU, Euratom) 2024/2509 van het Europees Parlement en de Raad van 23 september 2024 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie (herschikking) (PB L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

dwang, bijvoorbeeld door gebruik te maken van lock-ins ten aanzien van leveranciers of technologie, embargo's of sancties, monopolistische prijsstelling die de financiële belangen van de Unie en de lidstaten schaadt).

- (51) Om deze risico's aan te pakken en te voorzien in passende risicobeperkende maatregelen, is het noodzakelijk een Uniekader voor cloudcomputingsovereiniteit vast te stellen, waarin criteria voor betrouwbare cloudcomputingdiensten worden bepaald. Om recht te doen aan het genuanceerde en gelaagde karakter van soevereiniteit, moet het kader voorzien in vier verschillende niveaus van betrouwbaar aanbod ("Uniebetrouwbaarheidsniveaus").
- (52) De Uniebetrouwbaarheidsniveaus moeten voorzien in een evenredig kader om ervoor te zorgen dat de openbare orde wordt gehandhaafd door de controle en de zeggenschap bij overheidsinstanties te behouden. Voor de meeste openbare diensten geldt dat de hoogste betrouwbaarheidsniveaus niet noodzakelijk zijn. In bepaalde specifieke gevallen kan Uniebetrouwbaarheidsniveau 3 of 4 als noodzakelijk en evenredig worden beschouwd voor het handhaven van de openbare orde. De risicobeoordeling die door de lidstaten en de entiteiten van de Unie moet worden uitgevoerd, waarborgt dat de beginselen van evenredigheid en subsidiariteit worden nageleefd, door na te gaan in welke specifieke gevallen de bescherming van de openbare orde het hoogste betrouwbaarheidsniveau vereist.
- (53) Het is belangrijk dat de nationale bevoegde autoriteiten van vestiging van de aanbieder van cloudcomputingdiensten kunnen beoordelen of aanbieders van cloudcomputingdiensten die hun diensten aan entiteiten van de Unie en openbare lichamen in de Unie willen aanbieden, het juiste betrouwbaarheidsniveau bieden. Er is een mechanisme ingesteld voor de erkenning van cloudcomputingdiensten die ofwel beschikken over een EU-conformiteitsverklaring op basis van Uniebetrouwbaarheidsniveau 1, ofwel een "positief" controleadvies en controlerapport van een controleorganisatie hebben ontvangen. Zodra het erkenningsproces met een positief resultaat is afgerond, wordt de cloudcomputingdienst in de hele Unie erkend als een dienst die het vereiste Uniebetrouwbaarheidsniveau biedt. Met het oog op duidelijkheid, eenvoud en doeltreffendheid moeten de bevoegdheden voor het toezicht op en de handhaving van de verplichtingen in het kader van het kader voor cloudcomputingsovereiniteit worden toegekend aan de bevoegde autoriteiten in de lidstaat waar de hoofdvestiging van de aanbieder van cloudcomputingdiensten is gevestigd.
- (54) Om aan te tonen dat zij voldoen aan Uniebetrouwbaarheidsniveau 1, moeten aanbieders van cloudcomputingdiensten de volledige verantwoordelijkheid dragen voor het uitvoeren van conformiteitszelfbeoordelingen, waarbij zij de desbetreffende criteria voor dat Uniebetrouwbaarheidsniveau toepassen. Dergelijke zelfbeoordelingen moeten gebaseerd zijn op gedocumenteerd bewijsmateriaal, interne controleprocedures en voortdurende monitoring die toereikend zijn om aan te tonen dat aan de toepasselijke criteria is voldaan.
- (55) Onafhankelijke audits zijn een belangrijk instrument om na te gaan of cloudcomputingdiensten voldoen aan de gestelde eisen. Aangezien moet worden gewaarborgd dat de toepasselijke criteria voor Uniebetrouwbaarheidsniveau 2, 3 of 4 door onafhankelijke externe deskundigen worden gecontroleerd, moeten aanbieders van cloudcomputingdiensten via onafhankelijke audits verantwoording afleggen over de naleving van de in deze verordening vastgestelde criteria. Aanbieders van cloudcomputingdiensten moeten de vrijheid hebben om zelf een controleorganisatie te

kiezen, mits deze controleorganisatie aantoonst dat zij over de nodige onafhankelijkheid beschikt en voldoet aan de vereisten van deze verordening. Om ervoor te zorgen dat audits op een doeltreffende, efficiënte en tijdige wijze worden uitgevoerd, moeten aanbieders van cloudcomputingdiensten de nodige medewerking en bijstand verlenen aan de organisaties die de audits uitvoeren, onder meer door de controleorganisaties toegang te verlenen tot alle relevante gegevens en bedrijfsruimten die nodig zijn om de audit naar behoren uit te voeren, en door mondelinge of schriftelijke vragen te beantwoorden. Controleorganisaties moeten ook gebruik kunnen maken van andere bronnen van objectieve informatie. Aanbieders van cloudcomputingdiensten mogen de uitvoering van de audit niet ondermijnen. Audits moeten worden uitgevoerd volgens de beste praktijken in de sector en met grote beroepsethiek en objectiviteit, naar behoren rekening houdend met de controlenormen en gedragscodes. Controleorganisaties moeten de vertrouwelijkheid, veiligheid en integriteit van de informatie, zoals bedrijfsgeheimen, die zij bij de uitvoering van hun taken verkrijgen, waarborgen. Die waarborg mag geen middel zijn voor het omzeilen van de toepasselijkheid van controleverplichtingen in deze verordening. Controleorganisaties moeten beschikken over de nodige expertise op het gebied van risicobeheer en de technische bekwaamheid om cloudcomputingdiensten te controleren. Zij moeten voldoen aan de essentiële onafhankelijkheidsvereisten inzake het verbod op de aanbidding van andere diensten dan controlediensten, het wisselen van auditkantoor en niet-voorwaardelijke honoraria. Indien er twijfel bestaat over de onafhankelijkheid of de technische bekwaamheid van controleorganisaties, moeten zij zich van stemming onthouden of zich terugtrekken uit de controleopdracht.

- (56) Het controlerapport moet worden onderbouwd, zodat het een zinvolle rapportage geeft van de tijdens de audit ondernomen activiteiten en de bereikte conclusies. Dit moet bijdragen aan het verstrekken van informatie over, en waar nodig het voorstellen van verbeteringen aan, de maatregelen die de aanbieders van cloudcomputingdiensten hebben genomen om te voldoen aan de toepasselijke criteria en hun verplichtingen uit hoofde van deze verordening. Het controlerapport moet een controleadvies bevatten dat gebaseerd is op de conclusies die uit het verkregen controlebewijs worden getrokken. Er dient een “positief advies” te worden gegeven wanneer uit alle bewijsmateriaal blijkt dat de aanbieder voldoet aan de in deze verordening vastgestelde controlecriteria en verplichtingen. Er moet een “negatief advies” worden uitgebracht wanneer de controleorganisaties van mening zijn dat de aanbieder niet voldoet aan de in deze verordening vastgestelde criteria. Wanneer in het controleadvies geen conclusie kan worden getrokken over specifieke aspecten die binnen het toepassingsgebied van de audit vallen, moet in het controleadvies worden toegelicht waarom dit niet mogelijk was. In voorkomend geval moet het rapport een beschrijving bevatten van specifieke punten die niet konden worden gecontroleerd en een verklaring waarom dit niet mogelijk was.
- (57) De oprichting van een centraal register van erkende cloudcomputingdiensten die voldoen aan een van de Uniebetrouwbaarheidsniveaus is noodzakelijk om de veilige en efficiënte opslag, toegang tot en uitwisseling van relevante informatie te vergemakkelijken tussen klanten uit de publieke sector die gebruikmaken van diensten met een Uniebetrouwbaarheidsniveau, controleorganisaties, bevoegde autoriteiten en de Commissie.
- (58) Om ervoor te zorgen dat de status van cloudcomputingdiensten als diensten die overeenkomstig het kader voor cloudsoevereiniteit een Uniebetrouwbaarheidsniveau bieden, nauwkeurig en betrouwbaar blijft, moet van aanbieders worden verlangd dat

zij alle relevante informatie of essentiële wijzigingen in de omstandigheden onverwijld melden aan de controleorganisatie en de bevoegde autoriteiten van vestiging. Die informatie moet de controleorganisatie in staat stellen om het controlerapport en het advies indien nodig opnieuw te beoordelen, aan te passen of in te trekken, waarna de betrokken bevoegde autoriteit van vestiging hiervan in kennis wordt gesteld, zodat deze haar erkenning van de cloudcomputingdienst als een dienst die een bepaald Uniebetrouwbaarheidsniveau biedt, kan herzien. De informatie moet de bevoegde autoriteit in kwestie ook in staat stellen om de cloudcomputingdienst te erkennen.

- (59) Om een doeltreffende en consistente toepassing van het kader voor cloudsoevereiniteit te waarborgen, moeten de lidstaten een of meer bevoegde autoriteiten aanwijzen die verantwoordelijk zijn voor de erkenning van de controleprocedure en het controlekader, alsmede voor het toezicht op erkende aanbieders van cloudcomputingdiensten. Die autoriteiten moeten de nodige bevoegdheden, (technische) middelen en expertise krijgen om hun taken doeltreffend, onpartijdig en onafhankelijk uit te voeren. De lidstaten moeten ervoor zorgen dat de verantwoordelijkheden van deze autoriteiten duidelijk zijn vastgelegd en dat zij nauw samenwerken met elkaar, met andere betrokken nationale autoriteiten, waaronder gegevensbeschermings- en cyberbeveiligingsautoriteiten, en, waar nodig, met de Commissie, om een consistent toezicht te waarborgen en de uitwisseling van relevante informatie en beste praktijken in de hele Unie te vergemakkelijken. Het moet voor de lidstaten mogelijk zijn om één of meer bestaande autoriteiten aan te wijzen als bevoegde autoriteit(en).
- (60) De verlening van wederzijdse bijstand tussen bevoegde autoriteiten is essentieel om te zorgen voor een doeltreffend toezicht op en een doeltreffende handhaving van deze verordening over de grenzen van de Unie heen, onder meer door middel van tijdige uitwisseling van informatie, coördinatie van onderzoeksmaatregelen en ondersteuning bij de uitvoering van taken binnen de Unie. Bovendien vereist een doeltreffende handhaving een robuuste landsgrensoverschrijdende samenwerking tussen de bevoegde autoriteiten om te waarborgen dat deze verordening in alle lidstaten op consistente wijze wordt toegepast en dat relevante informatie tijdig wordt uitgewisseld om systeemrisico's binnen de Unie aan te pakken.
- (61) De doelstelling van de Unie om haar autonomie te versterken, moet worden nagestreefd op een manier die open en op samenwerking gericht blijft en in overeenstemming is met de internationale verplichtingen en partnerschappen van de Unie. De beleidsdoelstellingen die via de Uniebetrouwbaarheidsniveaus 1, 2 en 3 worden nagestreefd, moeten derhalve worden opgevat als het vermogen van de Unie om waar nodig autonoom op te treden, terwijl zij tegelijkertijd betrokken blijft bij haar internationale partners en wederzijds voordelige samenwerking bevordert. Tegen deze achtergrond kan de Commissie voor Uniebetrouwbaarheidsniveau 3 besluiten dat een cloudcomputingdienst die onder zeggenschap staat van een derde land of een in een derde land gevestigde rechtspersoon, toch aan de controlecriteria kan worden getoetst indien het derde land specifieke waarborgen heeft ingevoerd die ervoor zorgen dat er geen risico bestaat op ongeoorloofde toegang tot gegevens van de Unie of op een mogelijke verstoring van de kwaliteit of continuïteit van de dienst. De Commissie moet beoordelen of het derde land onder een overeenkomstig artikel 45 van Verordening (EU) 2016/679 vastgesteld adequaatheidsbesluit valt. Er moet met name worden vastgesteld of het adequaatheidsbesluit in het algemeen van toepassing is op het derde land als geheel, of dat het beperkt is tot specifieke sectoren of gecertificeerde organisaties. Er moet verder worden onderzocht of het toepassingsgebied van het

adequaatheidsbesluit zich uitstrekt tot de specifieke verwerkingsactiviteiten die in het kader van de dienstverlening worden uitgevoerd, of dat doorgiften onderworpen blijven aan de vereisten om passende waarborgen te treffen.

- (62) Om een samenhangende en op risico's gebaseerde benadering van de autonomie van de Unie te waarborgen, moeten de lidstaten en de entiteiten van de Unie een of meer risicobeoordelingen uitvoeren om vast te stellen welke activiteiten van de publieke sector betrekking hebben op de openbare orde. In de risicobeoordeling moet worden vastgesteld welk Uniebetrouwbaarheidsniveau passend is voor de activiteiten, gezien het belang ervan voor het handhaven van de openbare orde in sectoren die onder Richtlijn (EU) 2022/2555 vallen en op het gebied van nationale veiligheid, binnenlandse veiligheid, beheer van de buitengrenzen, defensie, justitie of wetshandhaving, zoals de preventie, het onderzoek, de opsporing en de vervolging van strafbare feiten. Om een consistente toepassing van deze verordening te waarborgen en de integriteit van de digitale eengemaakte markt te behouden, zal de Commissie richtsnoeren opstellen om de lidstaten te ondersteunen bij het uitvoeren van hun risicobeoordelingen. Hoewel het vaststellen van het gevoeligheidsniveau van informatie die mag worden gehost in een cloudcomputingdienst die een Uniebetrouwbaarheidsniveau biedt, onder de handelings- en de beoordelingsbevoegdheid van de lidstaten valt, moeten de Uniebetrouwbaarheidsniveaus 3 en 4, met het oog op consistentie in de hele Unie, de veilige hosting van gerubriceerde EU-informatie mogelijk maken.
- (63) In hun risicobeoordelingen moeten de entiteiten van de Unie en de lidstaten de gevoeligheid, de criticiteit en de omvang beoordelen van de persoonsgegevens en niet-persoonsgegevens die in een cloudomgeving worden verwerkt. Deze verwerking kan betrekking hebben op gewone bedrijfsinformatie, commercieel gevoelige informatie, operationeel kritieke gegevens, persoonsgegevens in de zin van Verordening (EU) 2016/679, en gegevens die onderworpen zijn aan sectorspecifieke verplichtingen krachtens het recht van de Unie, waaronder Richtlijn (EU) 2022/2555 en Verordening (EU) 2022/2554. De richtsnoeren van de Commissie bieden entiteiten van de Unie en de lidstaten een zekere mate van flexibiliteit bij het vaststellen van de passende Uniebetrouwbaarheidsniveaus en de categorieën informatie en gebruikers waarvoor dergelijke niveaus geschikt zijn. Tegelijkertijd kunnen uiteenlopende nationale benaderingen met betrekking tot het classificeren en in kaart brengen van de gevoeligheid van gegevens en de vereisten inzake betrouwbaarheid de consistente toepassing van het soevereiniteitskader in de hele Unie ondermijnen. Om een geharmoniseerde uitvoering in de hele Unie te waarborgen, moet de Commissie, in samenwerking met de bevoegde autoriteiten, centraal gecoördineerde richtsnoeren verstrekken inzake de koppeling tussen de Uniebetrouwbaarheidsniveaus en de categorieën informatie, waarbij rekening wordt gehouden met de gevoeligheid, criticiteit en omvang van de gegevens die door de cloudomgeving worden verwerkt, het systemische belang van de activiteiten van de aanbestedende diensten en de toepasselijke verplichtingen die voortvloeien uit het Unierecht. Bovendien mogen de criteria in het kader van de Uniebetrouwbaarheidsniveaus geen afbreuk doen aan de verplichtingen inzake landsgrensoverschrijdende samenwerking die in het Unierecht zijn vastgelegd. Wanneer cloudcomputingdiensten worden gebruikt voor de verwerking van persoonsgegevens, is in Verordening (EU) 2016/679 voorgeschreven dat er overeenstemming moet worden bereikt over organisatorische en technische maatregelen om aan die verordening te voldoen. Indien de aanbieder van cloudcomputingdiensten bij het verlenen van de diensten een beroep doet op subcontractanten, gelden dezelfde overeenkomsten ook voor de subcontractanten.

Wanneer op grond van deze verordening specifieke technische en organisatorische maatregelen moeten worden genomen om te waarborgen dat persoonsgegevens in overeenstemming met deze verordening worden verwerkt, kunnen dergelijke specifieke maatregelen worden opgenomen in de verplichte overeenkomsten op grond van Verordening (EU) 2016/679 en kunnen deze worden aangevoerd om aan te tonen dat aan de vereiste Uniebetrouwbaarheidsniveaus wordt voldaan.

- (64) Het vrije verkeer van gegevens binnen de Unie is een essentiële voorwaarde voor de goede werking van de interne markt. Om het vrije verkeer van gegevens binnen de Unie te bevorderen en de werking van de interne markt te ondersteunen, is het wenselijk dat de lidstaten ervoor zorgen dat gegevens niet beperkt blijven tot het grondgebied van één enkele lidstaat en zonder ongerechtvaardigde beperkingen in de hele Unie kunnen worden opgeslagen en verwerkt. De Unie handhaaft een open en niet-discriminerend kader voor markttoegang, in overeenstemming met het VWEU en met inachtneming van internationale verplichtingen. Daartoe behoren onder meer de verplichtingen uit hoofde van de Overeenkomst inzake overheidsopdrachten (GPA) van de Wereldhandelsorganisatie (WTO), evenals bilaterale handelsovereenkomsten. Niettemin behoudt de Unie, waar nodig en in naar behoren gemotiveerde gevallen, het recht om, overeenkomstig artikel III:2, punt a), van de GPA van de WTO, maatregelen vast te stellen of te handhaven die nodig zijn ter bescherming van de openbare zeden, orde of veiligheid, waarbij noodzakelijke en evenredige beperkingen op de toegang tot openbare aanbestedingsprocedures zijn toegestaan. Het opsporen en aanpakken van risico's zoals kritieke afhankelijkheden, ongeoorloofde toegang tot gegevens van de Unie, het lekken van technologie, sabotage en spionage door actoren uit derde landen is immers van fundamenteel belang voor het handhaven van de openbare orde in de Unie. Om de openbare orde van de Unie en haar lidstaten te beschermen, is een prudentiële maar krachtige politieke, juridische en operationele aanpak vereist voor aanbestedingsprocedures op zowel nationaal als Unieniveau, met volledige inachtneming van internationale verplichtingen. Om de openbare orde van de Unie en haar lidstaten te beschermen en te handhaven, moeten aanbestedende diensten waarvan de activiteiten op basis van de risicobeoordeling van de lidstaat zijn geïdentificeerd, derhalve uitsluitend gebruikmaken van cloudcomputingdiensten die een passend betrouwbaarheidsniveau bieden tussen niveau 2 en 4. Een minimum betrouwbaarheidsniveau, door in de hele Unie het Uniebetrouwbaarheidsniveau 1 verplicht te stellen, is noodzakelijk om een consistent basisniveau van waarborgen voor de publieke sector vast te stellen, waardoor de kwetsbaarheid van de publieke sector voor toegang door derde landen tot gegevens van de Unie en voor verstoring van de dienstverlening wordt verminderd.
- (65) Om de weerbaarheid te vergroten en de afhankelijkheid van één enkele aanbieder van cloudcomputingdiensten te beperken, moeten de entiteiten van de Unie en de lidstaten in het kader van hun openbare-aanbestedingsprocedures overwegen of een strategie met meerdere leveranciers of een multicloudstrategie geschikt zou kunnen zijn. Het besluit om een multicloudarchitectuur te gebruiken en in te voeren moet gebaseerd zijn op een contextspecifieke risicobeoordeling. Uit de beoordeling moet blijken of er relevante operationele, regelgevings- of weerbaarheidsgerelateerde omstandigheden zijn die het gebruik van een strategie met meerdere leveranciers of een multicloudstrategie zouden ondersteunen.
- (66) Overheidsopdrachten fungeren vaak als een belangrijke indicator voor de richting van de markt. Eisen die door of aan overheidsinstanties worden opgelegd om specifieke betrouwbaarheidsniveaus van cloudcomputingdiensten in te voeren, worden doorgaans

overgenomen door particuliere ondernemingen die actief zijn in gereguleerde sectoren, waarbij de daaruit voortvloeiende doorwerkingseffecten in de loop van de tijd bijdragen aan een bredere herschikking van de markt. Deze ontwikkelingen onderstrepen hoe belangrijk het is dat particuliere entiteiten die actief zijn in de in bijlage I bij Richtlijn (EU) 2022/2555 vermelde sectoren in staat zijn om dezelfde beoordelingen uit te voeren als die welke door entiteiten van de Unie en de lidstaten worden uitgevoerd.

- (67) Bij openbare aanbestedingsprocedures voor cloudcomputingdiensten en AI-systemen moeten aanbestedende diensten een duidelijke Europese meerwaarde opnemen als onderdeel van de kwaliteitsbeoordeling van de inschrijving. Die meerwaarde zou moeten bestaan uit het helpen versterken van de digitale toeleveringsketen in de Unie; het integreren van technologieën van de Unie; het doorvoeren van de innovatie die nodig is om de dienst in de Unie te verlenen, en het verlenen van de dienst met behulp van hardwarecomponenten die in de Unie zijn ontworpen of vervaardigd. Het criterium met betrekking tot de Europese meerwaarde mag niet doorslaggevend zijn voor de gunning van de opdracht en moet zodanig worden toegepast dat de voorrang van technische en financiële criteria die rechtstreeks verband houden met de prestatie-eisen, gewaarborgd blijft. Daartoe zouden aanbestedende diensten kunnen overwegen om binnen de algemene beoordelingsmethodologie een maximale weging van 15 van de 120 punten toe te kennen aan de Europese meerwaarde, waarbij zij ervoor zorgen dat deze weging evenredig blijft en ondergeschikt is aan de kerncriteria voor de gunning van de opdracht.
- (68) Innovatieve aanbestedingen op het gebied van cloudcomputingdiensten en AI-systemen zijn essentieel om technologische ontwikkeling te stimuleren, de digitale weerbaarheid en het concurrentievermogen te versterken en overheidsinstanties in staat te stellen te profiteren van veilige, efficiënte en betrouwbare digitale oplossingen die meegroeien met de snel veranderende technologische en maatschappelijke behoeften. De lidstaten zouden er daarom naar moeten streven om ten minste 25 % van de relevante aanbestedingsprocedures op het gebied van cloud en AI aan kmo's te gunnen. Daartoe moeten de lidstaten de Commissie actief informeren over hun gebruik van innovatieve cloudcomputingdiensten en AI-systemen.
- (69) In de gezamenlijke verklaring over de opbouw van clouddiensten van de volgende generatie cloud voor ondernemingen en de overheidssector in de EU van 15 oktober 2020³⁰ en de Verklaring van Berlijn van 8 december 2020 over een digitale samenleving en een op waarden gebaseerde digitale overheid³¹ hebben de lidstaten grote belangstelling geuit voor het vaststellen van een gemeenschappelijke aanpak voor het bundelen van cloudcapaciteiten door cloudinfrastructuur in de hele Unie met elkaar te verbinden en te werken aan de invoering van een veilige en interoperabele Europese cloudfederatie voor de publieke sector. In zijn conclusies over de toekomst van het digitale beleid van de EU van 21 mei 2024³² heeft de Raad van de Europese Unie het belang en de relevantie van het realiseren van deze gemeenschappelijke aanpak bevestigd door de Commissie te verzoeken haar steun voort te zetten voor de

³⁰ Gezamenlijke verklaring over de opbouw van clouddiensten van de volgende generatie cloud voor ondernemingen en de overheidssector in de EU, 15 oktober 2020, <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe> (Engelstalig).

³¹ Verklaring van Berlijn over een digitale samenleving en een op waarden gebaseerde digitale overheid, 8 december 2020, <https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government> (Engelstalig).

³² Conclusies van de Raad over de toekomst van het digitale beleid van de EU, 21 mei 2024, <https://data.consilium.europa.eu/doc/document/ST-9957-2024-INIT/nl/pdf>.

ontwikkeling van interoperabele openbare digitale diensten en de landsgrensoverschrijdende interconnectie van de infrastructuur van overheidsdiensten, zoals cloud- en edge-infrastructuur, teneinde de veerkracht, efficiëntie en duurzaamheid ervan te vergroten. Om deze gezamenlijke aanpak te realiseren, is het noodzakelijk om de Europese cloudfederatie voor de publieke sector (“Federatie EuroCloud”) op te richten. De Federatie EuroCloud moet nationale en Europese cloudinitiatieven samenbrengen die uiterst betrouwbare en veilige cloudcapaciteiten voor de publieke sector bieden en het delen van dergelijke capaciteiten tussen entiteiten van de Unie en overheidsinstanties vergemakkelijken. Bij de evaluatie van deze verordening kan de Commissie in een later stadium nagaan of toetredingslanden, kandidaat-lidstaten en potentiële kandidaat-lidstaten, alsook internationale organisaties waarvan het hoofdkantoor in de Unie is gevestigd, overeenkomstig het Unierecht kunnen deelnemen aan de Federatie EuroCloud.

- (70) De leden van de Federatie EuroCloud moeten aan specifieke vereisten voldoen om concurrentievervalsing ten opzichte van particuliere marktdeelnemers te voorkomen door een particuliere dienstverlener een bevoordeelde positie ten opzichte van zijn concurrenten te verlenen.
- (71) Deelname aan de Federatie EuroCloud moet beperkt blijven tot overheidsinstanties, zonder directe betrokkenheid van particuliere partijen. In dit verband moet directe particuliere deelname worden uitgesloten wanneer de delende entiteit, hetzij direct, hetzij indirect via een tussenliggende rechtspersoon, eigenaar is van de hardware, zoals gedefinieerd in artikel 3, punt 5, van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad³³, waarop de dienst beschikbaar wordt gesteld, en die dienst ook levert. De delende entiteit moet worden geacht zeggenschap uit te oefenen over die tussenliggende rechtspersoon wanneer aan de volgende cumulatieve voorwaarden is voldaan. Ten eerste moet de delende entiteit een doorslaggevende invloed uitoefenen op zowel de strategische doelstellingen als de belangrijke beslissingen van de tussenliggende rechtspersoon die eigenaar is van de hardware en de diensten levert. Ten tweede mag er geen directe deelname van particulier kapitaal in die tussenliggende rechtspersoon plaatsvinden. Ten derde moet meer dan 80 % van de activiteiten van de tussenliggende rechtspersoon worden verricht in het kader van de uitvoering van taken die haar door de delende entiteit zijn toevertrouwd.
- (72) Om een doeltreffende, veilige en weerbare dienstverlening te waarborgen, moet de delende entiteit passende technische, operationele en organisatorische maatregelen treffen. Dit moet met name beleid omvatten inzake risicoanalyse en de beveiliging van informatiesystemen, waaronder beleid inzake toegangscontrole, beleid inzake incidentafhandeling en bedrijfscontinuïteit en beleid ter ondersteuning van interoperabiliteit en connectiviteit.
- (73) Ten slotte moet het delen van datacentrumdiensten en cloudcomputingdiensten binnen de Federatie EuroCloud worden verankerd in een samenwerkingsverband binnen de publieke sector. Een dergelijke samenwerking moet uitsluitend worden ingegeven door overwegingen van algemeen belang en mag geen enkele vorm van tegenprestatie inhouden. In het bijzonder moet het delen van diensten binnen de Federatie EuroCloud kosteloos zijn, tenzij de kosten strikt beperkt blijven tot wat noodzakelijk en evenredig

³³ Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

is om de kosten te dekken die de delende entiteit maakt ten behoeve van de begunstigde gebruikende entiteit. Die kosten moeten beperkt blijven tot de extra kosten die voortvloeien uit het delen van capaciteit, zoals het toewijzen en afschermen van middelen, het beheren van de toegang, het mogelijk maken van de integratie en interoperabiliteit van middelen, het waarborgen van de naleving van de toepasselijke vereisten uit hoofde van het Unierecht en het beheren van de samenwerkingsrelatie. De vergoedingen die de delende entiteit in rekening brengt om deze kosten te dekken, mogen niet worden beschouwd als een tegenprestatie voor het verlenen van een dienst en mogen geen financieel belang of overheidsopdracht vormen in de zin van Richtlijn 2014/24/EU van het Europees Parlement en de Raad³⁴ en Verordening (EU, Euratom) 2024/2509. Onder die omstandigheden zou het delen van datacentrumdiensten en cloudcomputingdiensten van de publieke sector binnen de Federatie EuroCloud niet onder de regels van de Unie inzake overheidsopdrachten moeten vallen.

- (74) Aanbestedende diensten in de lidstaten ondervinden vaak aanzienlijke moeilijkheden bij de aanbesteding van digitale oplossingen, zoals datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen. Beperkte financiële middelen, verminderde koopkracht en onvoldoende technische of inkoopkennis beletten overheidsinstanties om daadwerkelijk gebruik te maken van dergelijke diensten. Aanbestedingsactiviteiten die de Commissie in overleg met de aanbestedende diensten van de lidstaten uitvoert, kunnen een doorslaggevende rol spelen bij het benutten van de collectieve koopkracht en het waarborgen van toegang tot die diensten en leveringen tegen gunstige voorwaarden. De Commissie kan reeds gezamenlijke aanbestedingsprocedures uitvoeren met aanbestedende diensten van de lidstaten overeenkomstig artikel 168, lid 2, van Verordening (EU, Euratom) 2024/2509. De Commissie kan ook al als groothandelaar optreden door goederen en diensten in te kopen, op voorraad te houden en door te verkopen of te schenken aan door haar geselecteerde partnerorganisaties. Om deze entiteiten in staat te stellen het potentieel van de interne markt ten volle te benutten, met name wat betreft schaalvoordelen en het delen van voordelen, moeten de mogelijkheden voor de Commissie om als aankoopcentrale op te treden, worden uitgebreid tot aanbestedende diensten van de lidstaten en tot door de Commissie geselecteerde partnerorganisaties, als een vorm van aanbesteding die een aanvulling vormt op de in artikel 168, lid 3, van Verordening (EU, Euratom) 2024/2509 genoemde vormen. De Commissie moet de mogelijkheid hebben om alle beschikbare aanbestedingsprocedures te gebruiken ten behoeve van de aanbestedende diensten van de lidstaten en van door de Commissie geselecteerde partnerorganisaties, en om aankoopactiviteiten die de Commissie uitvoert voor instellingen, organen en instanties van de Unie hierin op te nemen. Aanbestedende diensten van de lidstaten, partnerorganisaties en instellingen, organen en instanties van de Unie moeten in het kader van die aanbestedingsprocedures worden beschouwd als “deelnemende entiteiten”.
- (75) Om de flexibiliteit en de administratieve efficiëntie te vergroten, is het passend om, in afwijking van Verordening (EU, Euratom) 2024/2509, te voorzien in de mogelijkheid om tijdens de looptijd van een dynamisch aankoopstelsel deelnemende entiteiten toe te voegen. Op grond van die afwijking moet het deelnemende entiteiten die na de instelling van een dynamisch aankoopstelsel tot de overeenkomst zijn toegetreden,

³⁴ Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65, ELI: <http://data.europa.eu/eli/dir/2014/24/oj>).

worden toegestaan — mits de Commissie vooraf toestemming heeft verleend — om op elk moment tijdens de geldigheidsduur van dat systeem tot het systeem toe te treden, voordat een toekomstige uitnodiging tot inschrijving wordt bekendgemaakt. Die mogelijkheid moet strikt beperkt blijven tot nieuw toetredende deelnemende entiteiten en mag geen invloed hebben op de rechten en verplichtingen van entiteiten die reeds aan het systeem deelnemen, noch op de integriteit van reeds afgeronde of lopende aanbestedingsprocedures.

- (76) De Commissie moet de lidstaten een ontwerpovereenkomst voorleggen waarin de praktische regelingen voor de aanbestedingsactiviteiten worden vastgelegd. Gezien het mogelijk grote aantal betrokken deelnemende entiteiten, moet over die ontwerpovereenkomst worden onderhandeld en moet deze in eerste instantie worden gesloten tussen de Commissie en de lidstaten die bereid zijn deel te nemen. In de overeenkomst moeten de voorwaarden en de procedure worden vastgelegd op grond waarvan zowel entiteiten van de Unie als andere lidstaten, aanbestedende diensten van lidstaten en door de Commissie geselecteerde partnerorganisaties zich later bij deze overeenkomst kunnen aansluiten en ervan kunnen profiteren. De overeenkomst treedt in werking overeenkomstig de bepalingen daarvan, mits ten minste twee lidstaten deze goedkeuren. Hoewel de Commissie er zoveel mogelijk naar moet streven tegemoet te komen aan de gemeenschappelijke behoeften van de deelnemende entiteiten, mag dit niet worden opgevat als een verplichting om tegemoet te komen aan behoeften die specifiek zijn voor een beperkt aantal entiteiten.
- (77) Wanneer deelnemende entiteiten een overeenkomst sluiten voor het verrichten van gecentraliseerde aankoopactiviteiten, waaronder aanvullende aankoopactiviteiten, zouden zij de procedures voor overheidsopdrachten waarin de toepasselijke Uniewetgeving voorziet, overeenkomstig Richtlijn 2014/24/EU en Verordening (EU, Euratom) 2024/2509, niet mogen toepassen. Elke aanbestedende dienst uit een lidstaat die een dergelijke overeenkomst sluit met het oog op de organisatie van gecentraliseerde aankoopactiviteiten, moet worden geacht te voldoen aan zijn verplichtingen uit hoofde van de nationale wetgeving ter omzetting van Richtlijn 2014/24/EU, indien hij werken, leveringen of diensten afneemt van een aanbestedende dienst die verantwoordelijk is voor de aanbestedingsprocedure.
- (78) In de overeenkomst moet een stuurgroep worden ingesteld, bestaande uit de Commissie en vertegenwoordigers van de lidstaten. De stuurgroep is verantwoordelijk voor het strategisch toezicht op de aanbestedingsactiviteiten, inclusief de strategische sturing van de agenda van de openbare aanbestedingsactiviteiten en van elke aanbestedingsprocedure. De stuurgroep moet ook toezicht houden op de betrokkenheid van de deelnemende entiteiten. De stuurgroep mag niet verantwoordelijk zijn voor de uitvoering van aanbestedingsactiviteiten; dit moet onder de verantwoordelijkheid van de Commissie blijven vallen, zoals het vaststellen van vergoedingen. De stuurgroep moet zorgen voor de meest geschikte methode om extra vertegenwoordigers te selecteren uit entiteiten van de Unie, uit aanbestedende diensten van de lidstaten en uit door de Commissie geselecteerde partnerorganisaties.
- (79) In de overeenkomst moeten de regels inzake aansprakelijkheid en het toepasselijke kader voor overheidsopdrachten tussen de Commissie, die optreedt als aankoopcentrale, en de deelnemende entiteiten die via haar aankopen, worden verduidelijkt. Wanneer een deelnemende entiteit bepaalde onderdelen van de aanbestedingsprocedure zelfstandig uitvoert, dient deze de volledige verantwoordelijkheid te blijven dragen voor die fasen die zij zelfstandig uitvoert. Een aanbestedende dienst die als aankoopcentrale optreedt en diensten of goederen via de

Commissie heeft aangekocht, moet de mogelijkheid krijgen om die diensten aan andere aanbestedende diensten aan te bieden zonder de in het toepasselijke Unierecht vastgestelde procedures voor overheidsopdrachten toe te passen. In dat geval is de aanbestedende dienst verplicht om in elke volgende overeenkomst de oorspronkelijke contractuele bepalingen na te leven.

- (80) Om ervoor te zorgen dat de benodigde middelen beschikbaar blijven, zullen de deelnemende entiteiten bijdragen aan de kosten die voortvloeien uit de aanbestedingsprocedures en eventuele bijkomende activiteiten. Daartoe dient de Commissie het recht te hebben om vergoedingen in rekening te brengen bij de deelnemende entiteiten. Die vergoedingen moeten in beginsel zo worden vastgesteld dat zij toereikend zijn om alle directe en indirecte kosten te dekken die de Commissie in verband met de aanbestedingsactiviteiten maakt, inclusief eventuele aanvullende diensten. Die vergoedingen moeten worden vastgesteld in overeenstemming met de gangbare praktijken van vergelijkbare aanbestedingskaders. De initiële oprichtingskosten kunnen ten laste komen van de algemene begroting van de Unie en door de deelnemende entiteiten over een bepaalde periode worden terugbetaald. De ontvangsten uit de vergoedingen vormen interne bestemmingsontvangsten in de zin van artikel 21, lid 3, punt a), van Verordening (EU, Euratom) 2024/2509.
- (81) Opensource speelt een belangrijke rol bij het waarborgen van transparantie, veiligheid en efficiëntie bij het gebruik van digitale technologieën door de publieke sector. Toegang tot de broncode zorgt voor controleerbaarheid, bevordert samenwerking en hergebruik en vermindert de afhankelijkheid van één leverancier, waardoor het risico op afhankelijkheid van één leverancier wordt beperkt. Het bevorderen van het gebruik van opensource is dan ook essentieel om innovatie te ondersteunen, een betere rendabiliteit van de overheidsuitgaven te waarborgen en de digitale autonomie van de Unie te versterken. In dat verband heeft de keuze voor cloudcomputingdiensten of software niet alleen grote gevolgen voor de kostenefficiëntie, maar ook voor de veiligheid, de interoperabiliteit, de verantwoordingsplicht en de technologische autonomie.
- (82) Om een efficiënt, transparant en interoperabel gebruik van digitale technologieën binnen de hele publieke sector van de Unie te waarborgen, is het noodzakelijk dat overheidsinstanties bij het opzetten van hun cloud- en AI-ecosysteem of -stack open normen en componenten bevorderen die onder een opensourcelicentie worden vrijgegeven.
- (83) Steeds meer entiteiten van de Unie en overheidsinstanties delen software die door of voor hen is ontwikkeld en stellen deze onder een opensourcelicentie beschikbaar voor hergebruik. Dit kan worden beschouwd als zijnde in het algemeen belang en kan de waarde van de overheidsuitgaven maximaliseren, dubbele kosten verminderen en innovatie in de hele Unie bevorderen. Software wordt echter vaak in verschillende registers of catalogi beschikbaar gesteld en toegankelijk gemaakt, wat de doorzoekbaarheid, vindbaarheid en uiteindelijk het hergebruik bemoeilijkt. Het is daarom noodzakelijk om van entiteiten van de Unie en overheidsinstanties die vrijwillig besluiten software beschikbaar te stellen voor hergebruik, te eisen dat zij dit doen via een catalogus die of register dat is gekoppeld aan de EU-catalogus van opensourceoplossingen (“de EU-OSS-catalogus”). De EU-OSS-catalogus moet fungeren als een centrale catalogus voor alle openbare lichamen, waarmee zij software kunnen zoeken en raadplegen die door entiteiten van de Unie en openbare lichamen beschikbaar is gesteld voor hergebruik. Door de EU-catalogus van opensourceoplossingen te hosten op het Interoperabel Europa-portaal, zoals bedoeld in

artikel 8 van Verordening (EU) 2024/903³⁵, wordt ervoor gezorgd dat oplossingen gemakkelijk kunnen worden gekoppeld aan aanvullende relevante informatie en opleidingen.

- (84) Om te waarborgen dat de verplichtingen om een opensourcebeoordeling uit te voeren en software beschikbaar te stellen voor hergebruik in de hele Unie op doeltreffende en consistente wijze worden nageleefd, is het noodzakelijk een netwerk van opensourceprogrammabureaus (“het OSPO-netwerk”) op te zetten waarin de relevante structuren binnen de entiteiten van de Unie en de lidstaten worden samengebracht. Dit OSPO-netwerk moet de coördinatie bevorderen tussen opensourceprogrammabureaus die op lokaal, regionaal of nationaal niveau en door entiteiten van de Unie zijn opgericht. Het OSPO-netwerk moet de uitwisseling van informatie en beste praktijken faciliteren.
- (85) Om rekening te houden met de technologische ontwikkeling en een doelmatig kader van maatregelen te handhaven ter versterking van het cloud- en AI-ecosysteem op Unieniveau, moet aan de Commissie de bevoegdheid worden gedelegeerd om overeenkomstig artikel 290 VWEU handelingen vast te stellen in verband met: de wijziging van bijlage I om rekening te houden met relevante markt- en technologische ontwikkelingen met betrekking tot de initiatieven voor cloud- en AI-leiderschap en de wijziging van bijlage II om de criteria voor de Uniebetrouwbaarheidsniveaus te actualiseren; de aanvulling van deze verordening door nadere regels vast te stellen voor de uitvoering van audits; de wijziging van bijlage III; de vaststelling van een Uniebetrouwbaarheidsniveau voor een aanbestedende dienst, en het vereisen van een effectbeoordeling en risicobeperkende maatregelen voor particuliere ondernemingen die actief zijn in zeer kritieke sectoren.
- (86) Bij het vaststellen van gedelegeerde handelingen krachtens deze verordening is het van bijzonder belang dat de Commissie tijdens haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven³⁶. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen moeten het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip ontvangen als de deskundigen van de lidstaten, en moeten hun deskundigen altijd toegang hebben tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.
- (87) Om eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad³⁷.

³⁵ Verordening (EU) 2024/903 van het Europees Parlement en de Raad van 13 maart 2024 tot vaststelling van maatregelen voor een hoog niveau van interoperabiliteit van de overheidssector in de Unie (verordening Interoperabel Europa) (PB L, 2024/903, 22.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/903/oj>).

³⁶ Interinstitutioneel Akkoord tussen het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie over beter wetgeven (PB L 123 van 12.5.2016, blz. 1, ELI: http://data.europa.eu/eli/agree_interinst/2016/512/oj).

³⁷ Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

- (88) Gezien het belang van deze verordening voor de bescherming van persoonsgegevens moet de Europese Toezichthouder voor gegevensbescherming, indien nodig, worden geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725³⁸.
- (89) Indien een van de maatregelen waarin deze verordening voorziet staatssteun vormt, doen de bepalingen betreffende die maatregelen geen afbreuk aan de toepassing van de artikelen 107 en 108 VWEU.
- (90) Deze verordening laat de toepassing van de artikelen 101 en 102 VWEU en de handhavingsbevoegdheden van de mededingingsautoriteiten onverlet.
- (91) Daar de doelstellingen van deze verordening niet voldoende door de lidstaten kunnen worden verwezenlijkt, maar wegens de omvang of de gevolgen van het optreden beter door de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het VEU neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in dat artikel omschreven evenredigheidsbeginsel gaat deze verordening niet verder dan noodzakelijk is om dit doel te verwezenlijken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

³⁸ Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

TITEL I

ALGEMENE BEPALINGEN

Hoofdstuk I

Onderwerp en definities

Artikel 1

Onderwerp

1. Bij deze verordening wordt een kader vastgesteld voor de versterking van het cloud- en AI-ecosysteem op Unieniveau, met name middels de volgende maatregelen:
 - a) het instellen van het initiatief voor cloudleiderschap en het initiatief voor AI-leiderschap (“de initiatieven voor cloud- en AI-leiderschap”);
 - b) het vaststellen van het kader voor de versnelde uitrol van datacentra in de hele Unie;
 - c) het mogelijk maken van een soeverein aanbod van cloud en artificiële intelligentie (AI) ter bescherming van de openbare orde in de Unie;
 - d) het verminderen van de afhankelijkheid van kritieke technologieën;
 - e) het stimuleren van het gebruik van cloudcomputingdiensten in de hele publieke sector.
2. De eerste algemene doelstelling van deze verordening is het verzekeren van de nodige omstandigheden voor het concurrentievermogen en de innovatiecapaciteit van het cloud- en AI-ecosysteem van de Unie.
3. De tweede algemene doelstelling, die losstaat van en een aanvulling vormt op de in lid 2 bepaalde eerste algemene doelstelling, is de werking van de eengemaakte markt verbeteren door de vaststelling van een uniform Unierechtskader om de weerbaarheid en strategische autonomie van de Unie op het gebied van cloud- en AI-technologieën te versterken.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) “cloudcomputingdienst”: een cloudcomputingdienst zoals gedefinieerd in artikel 6, punt 30, van Richtlijn (EU) 2022/2555;
- 2) “aanbieder van cloudcomputingdiensten”: een juridische entiteit die een cloudcomputingdienst aanbiedt;
- 3) “AI-systeem”: een AI-systeem zoals gedefinieerd in artikel 3, punt 1, van Verordening (EU) 2024/1689;
- 4) “grensverleggende AI”: AI-modellen of op dergelijke modellen gebaseerde AI-systemen die een breed scala aan taken kunnen uitvoeren en die de huidige stand van de techniek benaderen, evenaren of overtreffen;
- 5) “AI-agent”: een AI-systeem dat of een gecoördineerde groep AI-systemen die de omgeving kan waarnemen en daarop kan reageren, met een zekere mate van

autonomie, waarbij naar behoefte gebruik wordt gemaakt van hulpmiddelen om specifieke doelen te bereiken en zich aan te passen aan veranderende input en contexten;

- 6) “openbaar lichaam”: een openbaar lichaam zoals gedefinieerd in artikel 2, punt 1, van Richtlijn (EU) 2019/1024;
- 7) “entiteiten van de Unie”: instellingen, organen en instanties van de Unie die zijn opgericht bij of krachtens het Verdrag betreffende de Europese Unie, het Verdrag betreffende de werking van de Europese Unie (VWEU) of het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie;
- 8) “kleine en middelgrote onderneming” of “kmo”: een kleine of middelgrote onderneming als omschreven in artikel 2 van bijlage I bij Aanbeveling 2003/361/EG van de Commissie;
- 9) “kleine midcap”: een kleine midcaponderneming als omschreven in punt 2 van de bijlage bij Aanbeveling (EU) 2025/1099 van de Commissie;
- 10) “datacentrum”: een datacentrum zoals gedefinieerd in punt 2.6.3.1.16 van bijlage A bij Verordening (EG) nr. 1099/2008 van het Europees Parlement en de Raad;
- 11) “exploitant van een datacentrum”: een exploitant van een datacentrum zoals gedefinieerd in artikel 2, punt 7, van Gedelegeerde Verordening (EU) 2024/1364;
- 12) “datacentrumdienst”: een datacentrumdienst zoals gedefinieerd in artikel 6, punt 31, van Richtlijn (EU) 2022/2555;
- 13) “software”: software zoals gedefinieerd in artikel 3, punt 4, van Verordening (EU) 2024/2847;
- 14) “hardware”: hardware zoals gedefinieerd in artikel 3, punt 5, van Verordening (EU) 2024/2847;
- 15) “component”: een component zoals gedefinieerd in artikel 3, punt 6, van Verordening (EU) 2024/2847;
- 16) “fabrikant”: een fabrikant zoals gedefinieerd in artikel 3, punt 13, van Verordening (EU) 2024/2847;
- 17) “controleorganisatie”: een afzonderlijke organisatie, een consortium of een andere combinatie van organisaties, waaronder eventuele subcontractanten, waarmee de gecontroleerde aanbieder van cloudcomputingdiensten een overeenkomst heeft gesloten voor het uitvoeren van een onafhankelijke audit;
- 18) “gecontroleerde dienst”: een cloudcomputingdienst die wordt gecontroleerd met het oog op het verkrijgen van een controlerapport en een controleadvies;
- 19) “controlecriteria”: de criteria, overeenkomstig bijlage II bij deze verordening, aan de hand waarvan de controleorganisatie beoordeelt of de gecontroleerde aanbieder en zijn gecontroleerde dienst voldoen aan elk cumulatief criterium waaraan moet worden voldaan om te worden erkend als aanbieder van Uniebetrouwbaarheidsniveau 2, 3 of 4;
- 20) “controlebewijs”: alle informatie die een controleorganisatie gebruikt ter onderbouwing van de controlebevindingen en -conclusies en voor het uitbrengen van een controleadvies, waaronder gegevens uit documenten, databanken of IT-systemen, gesprekken of uitgevoerde testen;

- 21) “zeggenschap”: zeggenschap zoals gedefinieerd in artikel 2, punt 6, van Verordening (EU) 2021/697;
- 22) “aanbestedende diensten”: aanbestedende diensten zoals gedefinieerd in artikel 2, lid 1, punt 1, van Richtlijn 2014/24/EU;
- 25) “opensourcelicentie”: een opensourcelicentie zoals gedefinieerd in artikel 2, punt 12, van Verordening (EU) 2024/903.

TITEL II

ONDERZOEK, ONTWIKKELING EN UITROLACTIVITEITEN VOOR HET CLOUD- EN AI- ECOSYSTEEM

Hoofdstuk I

Initiatieven voor cloud- en AI-leiderschap

Artikel 3

Algemene doelstelling van de initiatieven voor cloud- en AI-leiderschap

1. De initiatieven voor cloud- en AI-leiderschap hebben als algemene doelstelling het bevorderen van onderzoeks- en innovatieactiviteiten en het tot stand brengen van grootschalige capaciteit in het gehele cloud- en AI-ecosysteem van de Unie, door:
 - a) het ondersteunen van de ontwikkeling en uitrol van geavanceerde cloud- en AI-technologieën, waaronder de volgende generatie hulpbronnen efficiënte datacentrumtechnologieën, open technologieën voor cloudcomputingstack, grensverleggende AI en fysieke en industriële AI;
 - b) het versterken van de datacentrum- en cloudcapaciteit van de Unie om tegemoet te komen aan de groeiende vraag als gevolg van AI, innovatie te bevorderen en de weerbaarheid van de digitale infrastructuur te waarborgen;
 - c) het stimuleren van de vraag binnen de Unie en het bevorderen van de uitrol en het gebruik van cloud- en AI-technologieën in zowel de publieke als de particuliere sector, in overeenstemming met het digitale streefcijfer van de digitale transformatie van bedrijven, zoals vastgesteld bij Besluit (EU) 2022/2481.
2. Met de initiatieven voor cloud- en AI-leiderschap worden de volgende operationele doelstellingen nagestreefd:
 - a) het ondersteunen van de ontwikkeling en uitrol van geavanceerde datacentrumtechnologieën waarin beginselen van energie- en hulpbronnen efficiëntie zijn verwerkt, zowel in het ontwerp als gedurende de gehele exploitatie (operationele doelstelling 1);
 - b) het ondersteunen van de ontwikkeling en uitrol van cloudcomputingstacks die de technologische autonomie van de Unie bevorderen (operationele doelstelling 2);
 - c) het vergroten van de capaciteiten van de Unie op het gebied van grensverleggende AI (operationele doelstelling 3);
 - d) het versterken van de capaciteiten van de Unie op het gebied van fysieke AI-modellen en -systemen en het bevorderen van de toepassing daarvan in de strategische sectoren van de Unie (operationele doelstelling 4);
 - e) het versnellen van de ontwikkeling en toepassing van industriële AI in de strategische sectoren van de Unie (operationele doelstelling 5);

- f) het ondersteunen van de ontwikkeling van geavanceerde platforms voor de grootschalige inzet van AI-agenten (operationele doelstelling 6);
- g) het laten toenemen van de ontwikkeling en toepassing van AI-modellen en -systemen in de publieke sectoren van de Unie (operationele doelstelling 7);
- h) het vergroten van de toepassing van AI-technologieën op regionaal en lokaal niveau, en van het gebruik van cloudcomputingdiensten die worden aangeboden door Europese aanbieders van cloudcomputingdiensten (operationele doelstelling 8).

Artikel 4

Operationele doelstellingen van de initiatieven voor cloud- en AI-leiderschap

1. In het kader van operationele doelstelling 1 moeten de initiatieven voor cloud- en AI-leiderschap:
 - a) technologieën voor energie- en waterefficiëntie in datacentra, waaronder innovatieve koeling, datacentra van de volgende generatie op gelijkstroom, oplossingen voor het gebruik van restwarmte en energieopslagsystemen, verder ontwikkelen;
 - b) de integratie van opkomende kwantumcomputingtechnologieën bevorderen voor de exploitatie van cloud- en AI-computinginfrastructuur;
 - c) op AI gebaseerde technologieën ontwikkelen om de efficiëntie van servers, de bezettingsgraad en de werking van computinginfrastructuur te optimaliseren;
 - d) cloud- en edge-AI-infrastructuur ontwerpen en optimaliseren om een doeltreffende integratie met energienetten te waarborgen en de flexibiliteit ervan te vergroten;
 - e) datacentra inzetten als “anchor clients” voor geavanceerde energiebeheersystemen die gebruikmaken van diverse energiebronnen, waaronder kleine modulaire reactoren en schone waterstof, in combinatie met efficiënte oplossingen voor energieopslag;
 - f) testopstellingen en proeflijnen inzetten om de onder de punten a) tot en met e) ontwikkelde technologieën te integreren en te testen, waaronder energie-efficiënte prototypen op het gebied van halfgeleiders en kwantumcomputers.
2. In het kader van operationele doelstelling 2 zullen de initiatieven voor cloud- en AI-leiderschap:
 - a) veilige, weerbare en krachtige open cloudcomputingstacks ontwikkelen en testen die lagen voor edge-oplossingen op het apparaat zelf, connectiviteit, gegevens- en AI-hulpmiddelen, back-end en diensten omvatten voor strategische sectoren;
 - b) voor AI geoptimaliseerde servers en referentiesoftware ontwikkelen op basis van processoren, versnellers en kwantumversnellers die in de Unie zijn ontworpen en vervaardigd, naast gegevensopslag met ultrahoge dichtheid en voor de lange termijn van de volgende generatie;
 - c) de beschikbaarheid van gegevens voor AI vergroten via opensource-middlewareplatformen die ten grondslag liggen aan gemeenschappelijke Europese dataruimten;

- d) de ontwikkeling bevorderen van fundamentele opensourcesoftware die opensourcecomponenten ondersteunt;
 - e) een catalogus opstellen van Europese open cloudcomputingoplossingen die zijn ontwikkeld in het kader van de punten a) tot en met d) van dit lid.
3. In het kader van operationele doelstelling 3 ondersteunen de initiatieven voor cloud- en AI-leiderschap baanbrekende projecten op het gebied van grensverleggende AI, waarbij grensverleggende AI-modellen en -systemen als strategische activa worden ontwikkeld, onder meer in belangrijke sectoren zoals cyberbeveiliging.
4. In het kader van operationele doelstelling 4 zullen de initiatieven voor cloud- en AI-leiderschap:
- a) de ontwikkeling versnellen van een Europese fysieke AI-stack, ter ondersteuning van het trainen van modellen en de ontwikkeling en uitrol van systemen, met name voor robotica, autonome voertuigen en drones;
 - b) de toegang tot, en het verzamelen en opstellen van, specifieke datasets voor fysieke AI vergemakkelijken;
 - c) de ontwikkeling, het testen en de validatie van fysieke AI-modellen en -systemen in praktijkomgevingen ondersteunen.
5. In het kader van operationele doelstelling 5 zullen de initiatieven voor cloud- en AI-leiderschap:
- a) de ontwikkeling en toepassing van sectorale AI-modellen en -systemen in alle strategische industriële sectoren van de Unie versnellen;
 - b) de toegang vergemakkelijken tot de benodigde computingmiddelen en AI-hulpmiddelen die nodig zijn voor de ontwikkeling en ingebruikname van AI-modellen en -systemen die zijn afgestemd op de behoeften van de industriële sector;
 - c) veilige, grootschalige gegevensbundeling mogelijk maken voor gezamenlijke AI-training door middel van technologieën die de privacy versterken en de vertrouwelijkheid waarborgen.
6. In het kader van operationele doelstelling 6 zullen de initiatieven voor cloud- en AI-leiderschap:
- a) de ontwikkeling ondersteunen van geavanceerde, weerbare en veilige platformen voor de ontwikkeling, uitrol en coördinatie van geavanceerde AI-agenten op grote schaal;
 - b) de ontwikkeling bevorderen van gerichte test- en experimentele methoden voor geavanceerde AI-agenten en de coördinatie daarvan gedurende hun gehele levenscyclus.
7. In het kader van operationele doelstelling 7 zullen de initiatieven voor cloud- en AI-leiderschap:
- a) de technologische ontwikkeling en de toepassing van AI-modellen en -systemen in kritieke domeinen van de publieke sector versnellen;
 - b) AI-modellen en -systemen ontwikkelen die de doeltreffendheid van de openbare dienstverlening en de toegankelijkheid voor het grote publiek vergroten, de besluitvorming verbeteren en administratieve procedures vereenvoudigen;

- c) het delen en hergebruiken van trainingsdata en AI-modellen binnen de overheidsdiensten van de Unie bevorderen;
 - d) het hergebruik van gezondheidsgegevens voor AI-modellen en -hulpmiddelen in de gezondheidszorg op een veilige en privacybevorderende manier mogelijk maken;
 - e) de ontwikkeling, het testen en de uitrol van AI-modellen en -hulpmiddelen in de automobielsector faciliteren, onder meer op het gebied van autonoom rijden.
8. In het kader van operationele doelstelling 8 zullen de initiatieven voor cloud- en AI-leiderschap:
- a) de brede toepassing van AI door organisaties in de particuliere en publieke sector, waaronder kmo's en kleine midcaps, bevorderen via het netwerk van ervarings- en versnellingscentra voor AI ("centra voor AI");
 - b) een gemeenschappelijk leerplan voor cloud en AI ontwikkelen, waarbij gebruik wordt gemaakt van het netwerk van centra voor AI en andere relevante Europese initiatieven;
 - c) het delen van datacentrumdiensten en cloudcomputingdiensten in de publieke sector bevorderen door een Europese cloudfederatie voor de publieke sector ("Federatie EuroCloud") te ondersteunen;
 - d) de aankoop van datacentrumdiensten en cloudcomputingdiensten voor entiteiten van de Unie en openbare lichamen ondersteunen.

Artikel 5

Ervarings- en versnellingscentra voor AI

1. Elke lidstaat richt ervarings- en versnellingscentra voor AI ("centra voor AI") op. Die centra voor AI bouwen voort op de Europese digitale-innovatiehubs die zijn opgericht krachtens artikel 16 van Verordening (EU) 2021/694 en, indien van toepassing, op eventuele opvolgende entiteiten die krachtens het Unierecht zijn opgericht.
2. De centra voor AI hebben ten doel:
 - a) de ondersteuning van de integratie en opschaling van toepassingen van AI in strategische industriële en publieke sectoren;
 - b) de versnelling van de brede toepassing van cloud- en AI-technologieën op regionaal en lokaal niveau, met name voor kmo's, kleine midcaps en openbare lichamen, in overeenstemming met het AI-eerst-beginsel;
 - c) de aanwending van relevante infrastructuur om de ontwikkeling en verfijning van AI-modellen en -systemen te versnellen.
3. De centra voor AI krijgen met name de volgende taken toebedeeld:
 - a) organisaties helpen hun digitale transformatie te versnellen door middel van toegang tot en gebruik van AI-technologieën, onder meer door organisaties in contact te brengen met Europese aanbieders van cloud- en AI-technologieën;
 - b) het waarborgen of bieden van toegang tot relevante om- en bijscholingsprogramma's, in nauwe samenwerking met de academie voor AI-vaardigheden;

- c) het faciliteren van de overdracht van expertise tussen regio's;
 - d) het ondersteunen van de schaalvergroting van spin-offs en start-ups die voortkomen uit universiteiten, incubatoren en andere acceleratoren, door de toegang te vergemakkelijken tot klanten, ondernemingen en organisaties die op zoek zijn naar gespecialiseerde AI-diensten.
4. De Commissie kan uitvoeringshandelingen vaststellen waarin de procedure voor de oprichting van centra voor AI nader wordt uitgewerkt, evenals verdere bepalingen betreffende het profiel van de deelnemende organisaties, de selectiecriteria en nadere bepalingen inzake de uitvoering van de taken en functies. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.
 5. Centra voor AI beschikken over een aanzienlijke algemene autonomie wat betreft hun organisatie, samenstelling en werkwijzen, met inachtneming van de in deze verordening vastgestelde doelstellingen.
 6. Er wordt een netwerk van centra voor AI opgezet om de samenwerking en de uitwisseling van beste praktijken tussen centra voor AI te ondersteunen, en om gespecialiseerde diensten aan te bieden in regio's waar de benodigde vaardigheden of computingcapaciteit lokaal niet beschikbaar zijn.
 7. De lidstaten en de Commissie werken samen met bestaande netwerken die in het kader van andere initiatieven van de Unie zijn opgezet, waaronder initiatieven van de Unie op het gebied van halfgeleiders en data.

Artikel 6

Uitvoering van de initiatieven voor cloud- en AI-leiderschap

1. De uitvoering van de operationele doelstellingen van de initiatieven voor cloud- en AI-leiderschap wordt toevertrouwd aan de Commissie en de lidstaten en, indien van toepassing, aan gemeenschappelijke ondernemingen of andere structuren die in staat zijn deze doelstellingen te verwezenlijken.
2. De operationele doelstellingen van de initiatieven voor cloud- en AI-leiderschap worden verwezenlijkt door middel van grootschalige, sectoroverschrijdende initiatieven die gericht zijn op belangrijke technologische en industriële uitdagingen die van strategisch belang zijn voor de Unie ("grote uitdagingen"), zoals opgenomen in bijlage I.
3. De initiatieven voor cloud- en AI-leiderschap kunnen worden ondersteund met financiering uit programma's van de Unie, waaronder Horizon Europa en het programma Digitaal Europa, in overeenstemming met Verordening (EU) 2021/694 en Verordening (EU) 2021/695.
4. De Commissie is bevoegd om, ter aanpassing aan technologische veranderingen en marktontwikkelingen, in overeenstemming met artikel 45 gedelegeerde handelingen vast te stellen tot wijziging van bijlage I op een wijze die strookt met de specifieke doelstellingen van de initiatieven voor cloud- en AI-leiderschap, zoals opgenomen in artikel 4.

Artikel 7

Nationale cloud- en AI-strategieën

1. Uiterlijk op [de datum van inwerkingtreding plus één jaar] stellen de lidstaten nationale cloud- en AI-strategieën vast (de “nationale strategieën”).
2. De nationale strategieën omvatten ten minste het volgende:
 - a) de belangrijkste doelstellingen en prioriteiten voor de toepassing van cloud en AI, in overeenstemming met het AI-eerst-beginsel, evenals een kader voor governance en monitoring om die doelstellingen en prioriteiten te verwezenlijken;
 - b) maatregelen om de ontwikkeling en toepassing van cloud en AI op nationaal, regionaal en lokaal niveau te versnellen, met name bij openbare lichamen, kmo's en kleine midcaps, onder meer door de in artikel 5 bedoelde centra voor AI te ondersteunen als toegangspunten tot het Europese ecosysteem voor AI-innovatie;
 - c) maatregelen ter ondersteuning van de brede uitrol en toepassing van AI in strategische industriële en publieke sectoren, waaronder de gezondheidszorg, de energiesector en mobiliteit;
 - d) maatregelen ter ondersteuning van de uitrol van datacentrumcapaciteit, met bijzondere aandacht voor hoogwaardige datacentra die aanzienlijke economische en maatschappelijke voordelen opleveren en tegelijkertijd voldoen aan strenge milieu- en energie-efficiëntienormen;
 - e) maatregelen om te investeren in hoogintensieve computinginfrastructuur, waaronder AI-fabrieken, AI-gigafabrieken en kwantumcomputers, als strategische nationale en landsgrensoverschrijdende activa ter ondersteuning van onderzoek, ontwikkeling en de toepassing van industriële AI in strategische sectoren;
 - f) maatregelen ter ondersteuning van de ontwikkeling van cloud- en AI-capaciteiten en ter bevordering van excellentie en innovatie, onder meer door middel van maatregelen op het gebied van overheidsopdrachten, en maatregelen inzake innovatie bij overheidsopdrachten zoals bedoeld in artikel 33;
 - g) maatregelen ter ondersteuning van de ontwikkeling van cloudcomputingstacktechnologieën op basis van open hardware en software, teneinde de technologische soevereiniteit te versterken en het concurrentievermogen van strategische Europese industrieën te vergroten;
 - h) maatregelen om de toegankelijkheid van hoogwaardige gegevens voor de ontwikkeling van AI te waarborgen, met name door te voorkomen dat organisaties met gegevensknelpunten te maken krijgen.
3. Nationale strategieën moeten in overeenstemming zijn met de doelstellingen van deze verordening.
4. De lidstaten zorgen ervoor dat hun nationale strategieën in overeenstemming zijn met en bijdragen aan de desbetreffende digitale streefcijfers die zijn vastgesteld krachtens artikel 4 van Besluit (EU) 2022/2481.
5. De lidstaten brengen de nationale strategieën uiterlijk drie maanden na de vaststelling ervan ter kennis van de Commissie. De lidstaten beoordelen hun nationale

strategieën ten minste om de drie jaar op basis van kernprestatie-indicatoren, en werken deze zo nodig bij. De Commissie houdt toezicht op de vaststelling en herziening van de nationale strategieën.

6. De Europese raad voor artificiële intelligentie, opgericht bij Verordening (EU) 2024/1689 (de “AI-board”), adviseert en ondersteunt de lidstaten bij de coördinatie van nationale strategieën. De AI-board faciliteert de uitwisseling van beste praktijken tussen de lidstaten.

Artikel 8

Criteria voor prioritaire projecten op het gebied van grensverleggende AI

De Commissie kan bij besluit projecten die via openbare oproepen tot het indienen van blijken van belangstelling zijn geselecteerd en die bijdragen aan grote uitdaging 3, zoals uiteengezet in bijlage I, erkennen als prioritaire projecten op het gebied van grensverleggende AI, mits aan de volgende criteria wordt voldaan:

- a) het is een pioniersproject dat gericht is op de ondersteuning en opschaling van grensverleggende AI-technologieën;
- b) het wordt uitgevoerd door een Europees consortium voor digitale infrastructuur dat is opgericht krachtens Besluit (EU) 2022/2481 of door een andere juridische entiteit die op grond van het Unierecht in aanmerking komt voor financiering, en er zijn ten minste drie lidstaten bij betrokken;
- c) de deelnemende lidstaten stellen computingtijd en andere relevante middelen ter beschikking om de uitvoering van het aangewezen project te ondersteunen.

Artikel 9

Computingondersteuning voor AI-projecten

1. De Unie en de lidstaten zorgen ervoor dat, binnen de grenzen van de beschikbare capaciteit, voldoende AI-computingmiddelen uit hun computingcapaciteiten wordt toegewezen ter ondersteuning van de ontwikkeling van prioritaire projecten op het gebied van grensverleggende AI die voldoen aan de in artikel 8 vastgestelde criteria.
2. De Unie zal de door de lidstaten ter beschikking gestelde AI-computingmiddelen voor prioritaire projecten op het gebied van grensverleggende AI ten minste evenaren, voor zover er binnen het aandeel van de Unie in de Europese toegangstijd voor high-performance computing voldoende AI-computingcapaciteit beschikbaar is.
3. De Unie en de lidstaten streven ernaar voldoende computingmiddelen ter beschikking te stellen voor industriële innovatie op het gebied van AI, fysieke AI en AI-projecten in de publieke sector.

TITEL III

DATACENTRUMCAPACITEIT

Hoofdstuk I

Zones voor de versnelde uitrol van datacentra

Artikel 10

Aanwijzing van zones voor de versnelde uitrol van datacentra

1. Wanneer de capaciteit van datacentra op het grondgebied van een lidstaat wordt uitgerold, wijst die lidstaat uiterlijk op [P.O. insert the date of entry into force of this Regulation plus 6 months] ten minste één zone voor de versnelde uitrol van datacentra (“versnellingszone”) op zijn grondgebied aan. De lidstaten houden bij de aanwijzing van versnellingszones rekening met de volgende aspecten:
 - a) de plaats en omvang van de locatie of het gebied, en de minimum- en maximumomvang van de faciliteiten die op die locatie of dat gebied kunnen worden gebouwd;
 - b) de beschikbare en toekomstige capaciteit van het elektriciteitsnet en de mogelijkheden en voorwaarden voor opslag ter plaatse en opwekking van schone energie;
 - c) de beschikbare en toekomstige netwerkconnectiviteitscapaciteit;
 - d) de capaciteit van de zone om de uitfasering van oude kopernetwerken te ondersteunen;
 - e) de beschikbare en toekomstige faciliteiten die afvalwarmte van datacentra kunnen hergebruiken;
 - f) alle maatregelen die zijn genomen om de afgifte van de nodige vergunningen voor de bouw en exploitatie van datacentra binnen de desbetreffende zone te versnellen;
 - g) de voorkeur voor het hergebruik van brownfieldterreinen boven het gebruik van greenfieldterreinen;
 - h) het vermogen van de locatie of het gebied om voor duurzaam gebruik ervan, met name wat betreft het voorkomen of tot een minimum beperken van milieueffecten en het ondersteunen van de vermindering van koolstofemissies en de klimaatbestendigheid ervan.
2. De lidstaten moeten, in voorkomend geval om de ontwikkeling van versnellingszones te vergemakkelijken:
 - a) een uitgebreide analyse uitvoeren van de energiebehoeften en de respectieve effecten daarvan op de broeikasgasemissies van de huidige en toekomstige versnellingszones en deze ten minste om de drie jaar evalueren, en de vereiste energie-infrastructuurcapaciteit vaststellen voor de goede werking en ontwikkeling van datacentrumprojecten in de versnellingszones. Een dergelijke analyse wordt ten minste uitgevoerd bij de aanwijzing van de versnellingszones overeenkomstig lid 1;

- b) ervoor zorgen dat in de netwerkontwikkelingsplannen die door de transmissiesysteembeheerders overeenkomstig artikel 51 van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad en distributiesysteembeheerders overeenkomstig artikel 32 van Richtlijn (EU) 2019/944 worden opgesteld, naar behoren rekening wordt gehouden met de overeenkomstig punt a) van dit lid opgestelde analyse, rekening houdend met het potentieel van anticiperende investeringen om tegemoet te komen aan toekomstige systeembehoeften.
3. De nationale, regionale en lokale autoriteiten die verantwoordelijk zijn voor het opstellen van ruimtelijkeordenings- en ontwikkelingsplannen overwegen in die plannen bepalingen op te nemen voor de ontwikkeling van datacentrumprojecten die worden uitgerold in versnellingszones, en van de nodige infrastructuur. De lidstaten zorgen ervoor dat alle relevante gegevens inzake ruimtelijke ordening beschikbaar zijn voor exploitanten van datacentra. Indien die plannen onderworpen zijn aan een beoordeling overeenkomstig Richtlijn 2001/42/EG van het Europees Parlement en de Raad en artikel 6 van Richtlijn 92/43/EEG, worden die beoordelingen gecombineerd. In de gecombineerde beoordeling wordt in voorkomend geval ook ingegaan op de gevolgen voor mogelijk getroffen waterlichamen als genoemd in Richtlijn 2000/60/EG van het Europees Parlement en de Raad.
4. Bij de aanwijzing van versnellingszones zorgen de lidstaten ervoor dat alle relevante nationale, regionale en lokale autoriteiten en entiteiten, waaronder beheerders zoals gedefinieerd in artikel 2, punt 29), van Richtlijn (EU) 2018/1772 van het Europees Parlement en de Raad, transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35), van Richtlijn (EU) 2019/944 en distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 29), van Richtlijn (EU) 2019/944, hierbij worden betrokken en samenwerken.

Artikel 11

Omstandigheden binnen versnellingszones

1. Bij het vaststellen van duurzaamheidsvereisten voor datacentra die in versnellingszones worden uitgerold, gebruiken de lidstaten de kernprestatie-indicatoren die zijn gespecificeerd in Gedelegeerde Verordening (EU) 2024/1364, overeenkomstig bijlage II, punten a) tot en met n), bij Richtlijn (EU) 2023/1791.
2. De lidstaten zorgen ervoor dat de toewijzing en het gebruik van hulpbronnen binnen versnellingszones plaatsvinden op billijke, redelijke en niet-discriminerende voorwaarden en geen aanleiding geven tot speculatieve reserverings- of marktafschermingspraktijken die de daadwerkelijke mededinging of de doeltreffende ontwikkeling of het doeltreffende gebruik van die zones kunnen belemmeren.

Artikel 12

Centrale informatiepunten

1. De exploitant van het datacentrum heeft het recht om, op verzoek, gedurende de gehele levenscyclus van het datacentrumproject in een versnellingszone te worden bijgestaan door een centraal informatiepunt met betrekking tot alle vergunningen die vereist zijn voor de uitrol van het datacentrum. Daartoe wijzen de lidstaten één of meer centrale informatiepunten aan voor exploitanten van datacentra van datacentrumprojecten in versnellingszones. De lidstaten kunnen daartoe een uit hoofde van Verordening (EU) 2024/1309 opgericht centraal informatiepunt aanwijzen. De functies, procedures en mechanismen die van toepassing zijn op

dergelijke centrale informatiepunten uit hoofde van Verordening (EU) 2024/1309, waaronder die met betrekking tot digitale toegang, administratieve coördinatie en geschillenbeslechting, zijn ook van toepassing.

2. De rol van een centraal informatiepunt kan onder meer bestaan uit het coördineren, faciliteren, monitoren en delen van informatie over de procedure met betrekking tot:
 - a) ruimtelijke ordening en bouwvergunningen;
 - b) milieubeoordelingen, overeenkomstig Verordening (EU) 2026/XXXX [betreffende het versnellen van milieubeoordelingen];
 - c) vergunningen voor wateronttrekking, afvalwaterlozing en het gebruik en de terugwinning van afvalwarmte;
 - d) naleving van de toepasselijke administratieve en verslagleggingsverplichtingen;
 - e) publieksvoorlichting, met als doel het vergroten van het publieke draagvlak van het datacentrumproject;
 - f) toepassingen voor aansluiting op elektriciteitsnetten, verwarmingsnetwerken of communicatienetwerken of op andere relevante netwerken.
3. Het centrale informatiepunt helpt bij de beoordeling of een datacentrumproject kan worden aangemerkt als een strategisch project uit hoofde van artikel 14.
4. Bij het verlenen van de in dit artikel bedoelde administratieve ondersteuning en bijstand besteedt het centrale contactpunt bijzondere aandacht aan kmo's en zet het, in voorkomend geval, een specifiek kanaal op voor communicatie met kmo's om richtsnoeren te verstrekken en vragen in verband met de uitvoering van deze verordening te beantwoorden.

Artikel 13

Faciliteren van administratieve en vergunningsprocedures

1. Datacentrumprojecten die worden uitgerold in versnellingszones worden beschouwd als strategische projecten in de zin van artikel 14 van Verordening (EU) 2026/XXX [betreffende het versnellen van milieubeoordelingen] en komen in aanmerking voor de in de bijlage bij die verordening vastgestelde toolbox.
2. Voor elke aangewezen versnellingszone wordt door de lidstaten een geaggregeerde basisvergunning opgesteld en afgegeven, waarmee de uitrol van datacentra in die versnellingszone wordt toegestaan. Deze geaggregeerde basisvergunning bestrijkt de vergunningen en administratieve machtigingen die noodzakelijk zijn voor de datacentrumprojecten in die versnellingszone, met uitzondering van installatiespecifieke vergunningen.
3. Alvorens de in lid 2 bedoelde geaggregeerde basisvergunning af te geven, voeren de lidstaten alle nodige procedures en beoordelingen uit, waaronder relevante milieubeoordelingen, planningsprocedures en evaluaties die van toepassing zijn op het niveau van de versnellingszone.
4. Datacentra die in versnellingszones worden uitgerold, hebben alleen aanvullende vergunningen nodig voor activiteiten die buiten de in lid 2 bedoelde geaggregeerde basisvergunning vallen.

5. De lidstaten zorgen ervoor dat administratieve aanvragen met betrekking tot de planning, de bouw en de exploitatie van datacentra die in versnellingszones worden uitgerold, op een efficiënte en transparante wijze en tijdig worden verwerkt. De vergunningsprocedure voor datacentrumprojecten die worden uitgerold in versnellingszones duurt niet langer dan 12 maanden, te rekenen vanaf het moment waarop een uitgebreide aanvraag is ingediend. Deze termijn laat eventuele kortere termijnen die door de lidstaten zijn vastgesteld, onverlet. Indien het nationaal recht een dergelijke status erkent, wordt aan datacentrumprojecten de hoogst mogelijke status van nationaal belang verleend en worden zij als zodanig behandeld in vergunningsprocedures. Dit lid geldt alleen wanneer het nationaal recht een dergelijke status kent en brengt voor de lidstaten niet de verplichting met zich mee om een dergelijke status in te voeren.

Hoofdstuk II

Strategische projecten

AFDELING 1

AANWIJZING VAN STRATEGISCHE DATACENTRUMPROJECTEN

Artikel 14

Aanwijzing van strategische datacentrumprojecten

1. De Commissie kan bij besluit datacentrumprojecten die zijn geselecteerd via openbare oproepen tot het indienen van blijken van belangstelling en die aan ten minste twee van de volgende criteria voldoen, als strategische projecten aanwijzen:
- a) het project zorgt voor het tot stand brengen en exploiteren van infrastructuur die essentiële overheidsfuncties, waaronder onderzoek en onderwijs, gezondheidszorg, openbare veiligheid en beveiliging, rechtstreeks ondersteunt en versterkt;
 - b) het project heeft zeer duurzame of innovatieve kenmerken, waaronder technologieën en oplossingen die in het kader van titel II zijn ontwikkeld;
 - c) het project draagt bij tot de beveiliging, veiligheid en stabiliteit van het elektriciteitsnet en tot de behoeften van het elektriciteitssysteem zoals beoordeeld door de relevante systeembeheerder, met name voor projecten die betrekking hebben op de colocatie van grote installaties voor de opwekking en opslag van schone energie;
 - d) het project ondersteunt de integratie van in de Unie ontworpen en/of vervaardigde chips, processoren en versnellers, servers of kwantumcomputers in het beheer van datacentrumsystemen of van datacentrumfaciliteiten, waardoor de toeleveringsketens van de Unie voor halfgeleiders, kwantumtechnologie en datacentra worden versterkt en wordt bijgedragen tot de doelstellingen van deze verordening en van Verordening (EU) 2023/1781;
 - e) het project pakt een groot tekort aan rekencapaciteit aan in een gebied waarvoor een dergelijk tekort is vastgesteld op grond van artikel 15 en draagt aanzienlijk bij tot de groei, ontwikkeling en bevordering van de lokale economie.

2. In zijn voorstel verstrekt de aanvrager alle noodzakelijke en relevante informatie om aan te tonen dat het project aan de relevante criteria voldoet.
3. De duur van de aanwijzing als strategisch project wordt gebaseerd op de verwachte levensduur van het project. De aanvrager neemt in het voorstel de informatie op die nodig is om de voorspelde levensduur van het project te onderbouwen, op basis waarvan de duur van de aanwijzing als strategisch project wordt bepaald.
4. Indien de Commissie vaststelt dat een als strategisch project aangewezen project niet langer aan de relevante criteria voldoet, of indien de aanwijzing ervan was gebaseerd op een aanvraag die onjuiste informatie bevat die van invloed is op de naleving van die criteria, kan zij de aanwijzing van dat project bij besluit intrekken. Projecten waarvoor de aanwijzing als strategisch project is ingetrokken, verliezen alle rechten in verband met die status uit hoofde van deze verordening.

Hoofdstuk III

Monitoring

Artikel 15

Monitoring van het capaciteitstekort

1. Met het oog op de monitoring van de vooruitgang bij de verwezenlijking van de doelstellingen van Besluit (EU) 2022/2481 identificeert en monitort de Commissie:
 - a) de in de Unie beschikbare rekencapaciteit, inclusief edgecomputingcapaciteit;
 - b) het volume van de vraag naar datacentrumcapaciteit;
 - c) de omvang van het capaciteitstekort en gebieden met onvoldoende dekking die door de Commissie, in samenwerking met de lidstaten, kunnen worden geïdentificeerd en vervolgens kunnen worden gebruikt als versnellingszones voor de uitrol van datacentrumcapaciteit.

TITEL IV AUTONOMIE

Hoofdstuk I Soevereiniteitskader voor cloudcomputing

AFDELING 1 UNIEBETROUWBAARHEIDSNIVEAUS

Artikel 16

Toepassingsgebied

1. Bij dit hoofdstuk wordt een Uniekader voor cloudcomputingsoevereiniteit vastgesteld dat vier Uniebetrouwbaarheidsniveaus omvat, waarvoor de criteria in bijlage II zijn vastgesteld, waaraan aanbieders van cloudcomputingdiensten moeten voldoen om hun cloudcomputingdiensten aan entiteiten van en openbare lichamen in de Unie aan te bieden.
2. De Commissie is bevoegd overeenkomstig artikel 45 gedelegeerde handelingen vast te stellen om de in bijlage II vermelde Uniebetrouwbaarheidsniveaus en het in bijlage III vermelde bewijsmateriaal te wijzigen.
3. Om ervoor te zorgen dat bijlagen II en III actueel blijven en worden aangepast aan nieuwe juridische of technische ontwikkelingen, evalueert de Commissie deze ten minste om de 18 maanden.

Artikel 17

Erkenning van aanbieders van cloudcomputingdiensten

1. Een aanbieder van cloudcomputingdiensten die wil worden erkend als aanbieder van een Uniebetrouwbaarheidsniveau, dient een erkenningsaanvraag in bij de nationale bevoegde autoriteit van vestiging. Bij de indiening van een erkenningsaanvraag voegt de aanbieder van cloudcomputingdiensten alle krachtens lid 3 of lid 4 vereiste relevante bewijsstukken toe.
2. De bevoegde autoriteit van vestiging is de beoordelende nationale bevoegde autoriteit. Een beoordelende nationale bevoegde autoriteit die een aanvraag voor een kandidaat-erkenning heeft ontvangen, kan, indien nodig, een of meer bevoegde autoriteiten van de andere lidstaten verzoeken om mee te werken aan de procedure voor een kandidaat-erkenning uit hoofde van dit artikel. Binnen 15 dagen na ontvangst van een dergelijk verzoek bevestigt de nationale autoriteit die een verzoek om samenwerking heeft ontvangen dat zij ermee instemt met de beoordelende nationale bevoegde autoriteit samen te werken, of weigert zij het verzoek.
3. Voor Uniebetrouwbaarheidsniveau 1 overlegt de kandidaat-aanbieder van cloudcomputingdiensten bij de beoordelende nationale bevoegde autoriteit de in artikel 19, lid 2, bedoelde EU-conformiteitsverklaring en alle nodige bewijsstukken.

In afwijking van de eerste alinea worden EU-conformiteitsverklaringen die uit hoofde van artikel 19, lid 2, worden overgelegd door aanbieders van cloudcomputingdiensten die kmo's zijn, rechtstreeks en automatisch erkend in alle

lidstaten zonder dat voorafgaande erkenning door de beoordelende nationale bevoegde autoriteit nodig is.

4. Voor Uniebetrouwbaarheidsniveaus 2, 3 en 4 overlegt de kandidaat-aanbieder van cloudcomputingdiensten bij de beoordelende nationale bevoegde autoriteit het controlerapport, het in artikel 20 bedoelde “positieve” controleadvies en alle tijdens de controleprocedure aan de controleorganisatie verstrekte bewijstukken.
5. Binnen 60 dagen na aanvaarding van een aanvraag overeenkomstig lid 1 beoordeelt de beoordelende nationale bevoegde autoriteit het overeenkomstig lid 3 of lid 4 overgelegde bewijsmateriaal en:
 - a) stelt zij een ontwerperkenningsbesluit op en stelt zij de bevoegde autoriteiten van de andere lidstaten hiervan zo spoedig mogelijk in kennis, zodat zij gedurende een beoordelingsperiode van zestig dagen kunnen reageren op haar voornemen om de cloudcomputingdienst in de hele Unie te erkennen als een dienst die het toepasselijke Uniebetrouwbaarheidsniveau biedt. De kennisgeving van de beoordelingstermijn aan de bevoegde autoriteiten van de andere lidstaten bevat het in lid 3 of lid 4 bedoelde bewijsmateriaal, of
 - b) kan, indien het ingediende bewijsmateriaal ontoereikend is om de beoordelende bevoegde autoriteit in staat te stellen de cloudcomputingdienst te erkennen, de aanvrager om nadere informatie verzoeken en hem verzoeken die informatie binnen een bepaalde termijn in te dienen. De in dit lid bedoelde periode van zestig dagen wordt opgeschort vanaf de datum waarop het verzoek wordt gedaan tot de datum waarop de informatie is ontvangen. De opschorting mag niet langer dan 30 dagen duren, tenzij de aard van de gevraagde informatie of uitzonderlijke omstandigheden dit rechtvaardigen, of
 - c) wijst het verzoek om erkenning af. Alvorens het verzoek om erkenning af te wijzen, stelt de beoordelende bevoegde autoriteit de kandidaat-aanbieder van cloudcomputingdiensten in de gelegenheid binnen 30 dagen schriftelijke opmerkingen over de conclusies van de beoordeling in te dienen. De beoordelende bevoegde autoriteit houdt bij het opstellen van de definitieve conclusie terdege rekening met deze opmerkingen.
6. Tijdens de in lid 5, punt a), bedoelde beoordelingstermijn kan de nationale bevoegde autoriteit van een andere lidstaat bij de beoordelende nationale bevoegde autoriteit een met redenen omkleed bezwaar of verzoek om verduidelijking indienen indien zij van oordeel is dat het ontwerperkenningsbesluit niet in overeenstemming is met het toepasselijke Uniebetrouwbaarheidsniveau als vermeld in bijlage II.
7. Indien binnen de in lid 5, punt a), bedoelde beoordelingstermijn geen met redenen omkleed bezwaar of verzoek om verduidelijking is ingediend, worden de conclusies van de beoordelende nationale bevoegde autoriteit geacht door alle lidstaten te zijn aanvaard, stelt de beoordelende nationale bevoegde autoriteit het erkenningsbesluit vast en wordt de gecontroleerde dienst in de hele Unie erkend op het passende Uniebetrouwbaarheidsniveau.
8. Indien binnen de in lid 5, punt a), bedoelde beoordelingstermijn een verzoek om verduidelijking wordt ingediend, houdt de beoordelende nationale bevoegde autoriteit terdege rekening met dat verzoek en verzoekt zij, in voorkomend geval, de aanvrager om nieuwe informatie overeenkomstig lid 5, punt b), of bevestigt of wijzigt zij haar oorspronkelijke ontwerpbesluit. Indien de verzoekende bevoegde autoriteit niet overtuigd is, kan zij een met redenen omkleed bezwaar indienen.

9. Indien binnen de in lid 5, punt a), bedoelde beoordelingstermijn of volgens de in lid 8 bedoelde procedure een gemotiveerd bezwaar wordt ingediend, beoordeelt de beoordelende nationale bevoegde autoriteit het bezwaar en handhaaft zij haar oorspronkelijke ontwerpbesluit of trekt zij dit in. De beoordelende nationale bevoegde autoriteit stelt de bevoegde autoriteiten van de andere lidstaten daarvan in kennis binnen 15 dagen na het einde van de in lid 5, punt a), bedoelde beoordelingstermijn of binnen 15 dagen na ontvangst van het gemotiveerde bezwaar volgens de in lid 8 bedoelde procedure, naargelang het geval.
10. Indien de beoordelende nationale bevoegde autoriteit voornemens is haar ontwerpbesluit te handhaven, kan de betrokken nationale bevoegde autoriteit de zaak voorleggen aan de Commissie. De Commissie beoordeelt de zaak en kan de betrokken nationale bevoegde autoriteiten om informatie verzoeken. De Commissie stelt een bindend besluit vast waarin wordt bepaald of de beoordelende nationale bevoegde autoriteit het erkenningsbesluit mag vaststellen.
11. De beoordelende nationale bevoegde autoriteit kan haar erkenning intrekken indien zij vaststelt dat een aanbieder van cloudcomputingdiensten van wie de dienst in de hele Unie is erkend als aanbieder van een specifiek Uniebetrouwbaarheidsniveau, opzettelijk of uit onachtzaamheid onjuiste of misleidende informatie heeft verstrekt.
12. De Commissie kan uitvoeringshandelingen vaststellen met betrekking tot de praktische regelingen voor de in dit artikel bedoelde procedures. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.
13. Om de haar krachtens lid 10 toegewezen taken uit te voeren, kan de Commissie van de nationale bevoegde autoriteiten van vestiging verlangen dat zij zo spoedig mogelijk en binnen een redelijke termijn alle relevante informatie over de betrokken aanbieder van cloudcomputingdiensten en de erkenningsaanvraag verstrekken.
14. Bij het indienen van een verzoeken om informatie vermeldt de Commissie het doel van het verzoek, specificeert welke informatie wordt verlangd en stelt de termijn vast waarbinnen de informatie moet worden verstrekt.

Artikel 18

Geassocieerde derde landen

1. De Commissie kan door middel van uitvoeringshandelingen besluiten vaststellen om derde landen te identificeren waarvoor, in het geval dat de aanbieders van cloudcomputingdiensten onder zeggenschap van dat derde land staan of van een in dat derde land gevestigde juridische entiteit staan, die aanbieders kunnen worden gecontroleerd aan de hand van de criteria voor Uniebetrouwbaarheidsniveau 3 overeenkomstig bijlage II, mits dat derde land aan elk van de volgende criteria voldoet:
 - a) het is onderworpen aan een relevant adequaatheidsbesluit dat is vastgesteld op grond van artikel 45 van Verordening (EU) 2016/679;
 - b) het heeft geen maatregelen genomen die het land in staat stellen zeggenschap uit te oefenen over de aanbieder van cloudcomputingdiensten op een wijze die in strijd zou zijn met de vereisten voor rechtmatige toegang tot niet-persoonsgebonden gegevens als bedoeld in artikel 32, leden 2 en 3, van Verordening (EU) 2023/2854;

- c) het heeft geen maatregelen genomen om de aanbieder van cloudcomputingdiensten te dwingen de continuïteit of verlening van de dienst aan te tasten of te verstoren. Het heeft evenmin maatregelen genomen om de aanbieder van cloudcomputingdiensten te verplichten beperkende maatregelen, zoals sanctieregelingen, embargo's of gelijkwaardige wettelijke of bestuursrechtelijke maatregelen, uit te voeren, te handhaven of na te leven, tenzij deze specifieke maatregelen rechtmatig zijn uit hoofde van het nationale recht van de lidstaten of het Unierecht;
- d) het heeft geen maatregelen genomen om de levering van geavanceerde technologieën en diensten door de aanbieder van cloudcomputingdiensten te belemmeren;
- e) het handhaaft een open markt voor EU-cloudcomputingdiensten;
- f) het derde land verleent gelijkwaardige niveaus van toegang tot openbare aanbestedingsprocedures voor cloudcomputingdiensten die onder zeggenschap staan van een EU-lidstaat of entiteit in de Unie of een in de Unie gevestigde juridische entiteit.

Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

- 2. Indien uit de beschikbare informatie blijkt dat het derde land niet langer aan de vereisten van lid 1 voldoet, trekt de Commissie het in lid 1 bedoelde besluit in, wijzigt zij het of schorst zij het.
- 3. De Commissie publiceert op haar website een lijst van derde landen die aan de vereisten van lid 1 voldoen en van derde landen die daar niet langer aan voldoen.

AFDELING 2

CONFORMITEITSBEOORDELINGSPROCEDURES

Artikel 19

Conformiteitszelfbeoordeling

- 1. Aanbieders van cloudcomputingdiensten die overeenkomstig artikel 17 erkenning aanvragen als aanbieders van Uniebetrouwbaarheidsniveau 1, voeren een conformiteitszelfbeoordeling uit van de naleving van de criteria voor Uniebetrouwbaarheidsniveau 1 als vastgesteld in bijlage II.
- 2. Na de in lid 1 bedoelde zelfbeoordeling overlegt de aanbieder van cloudcomputingdiensten een EU-conformiteitsverklaring waarin wordt verklaard dat de naleving van de criteria voor Uniebetrouwbaarheidsniveau 1 is aangetoond. Door een dergelijke verklaring te overleggen, neemt de aanbieder van cloudcomputingdiensten de verantwoordelijkheid op zich voor de naleving door de cloudcomputingdienst van de criteria voor Uniebetrouwbaarheidsniveau 1 als vastgesteld in bijlage II.
- 3. De aanbieder van cloudcomputingdiensten maakt de EU-conformiteitsverklaring openbaar.

AFDELING 3

CONTROLE DOOR EEN ONAFHANKELIJKE DERDE

Artikel 20

Onafhankelijke controle

1. Aanbieders van cloudcomputingdiensten die overeenkomstig artikel 17 willen worden erkend als aanbieders van Uniebetrouwbaarheidsniveau 2, 3 of 4, ondergaan op eigen kosten controle door een onafhankelijke derde om een controlerapport en een controleadvies van een controleorganisatie te verkrijgen. Een gecontroleerde aanbieder die een controleprocedure voor een hoger Uniebetrouwbaarheidsniveau ondergaat, voldoet aan alle toepasselijke cumulatieve criteria van bijlage II die van toepassing zijn op de lagere Uniebetrouwbaarheidsniveaus. Indien niet aan de vereisten van een lager zekerheidsniveau wordt voldaan, is conformiteit met de hogere Uniebetrouwbaarheidsniveaus uitgesloten.
2. Gecontroleerde aanbieders werken samen met controleorganisaties en verlenen hun de nodige bijstand om hen in staat te stellen die controles op een doeltreffende en efficiënte wijze en tijdig uit te voeren, onder meer door hun toegang te verlenen tot alle relevante gegevens en bedrijfsruimten en door mondelinge of schriftelijke vragen te beantwoorden. De gecontroleerde aanbieders onthouden zich ervan de uitvoering van de controle te belemmeren, onnodig te beïnvloeden of te ondermijnen.
3. Controleorganisaties waarborgen een passend niveau van vertrouwelijkheid en beroepsgeheim met betrekking tot de informatie die zij in het kader van de controles van de gecontroleerde aanbieders en derden hebben verkregen, ook na afloop van de controles. Deze eis mag geen negatieve invloed hebben op de uitvoering van de controles en andere bepalingen van deze verordening. Op grond van artikel 23 deelt de controleorganisatie alleen informatie die nodig is voor de verslaglegging en die geen informatie bevat die redelijkerwijs als vertrouwelijk kan worden beschouwd.
4. De in lid 1 bedoelde controles worden uitgevoerd door controleorganisaties die:
 - a) onafhankelijk zijn van en geen belangenconflicten hebben met de betrokken aanbieder van cloudcomputingdiensten en met die aanbieder verbonden rechtspersonen, en die met name:
 - i. in de periode van twaalf maanden vóór aanvang van de controle geen niet-controlediensten met betrekking tot de gecontroleerde aangelegenheden hebben verleend aan de betrokken aanbieder van cloudcomputingdiensten of aan een met die aanbieder verbonden rechtspersoon, en zich ertoe hebben verbonden deze diensten niet te verlenen in de periode van twaalf maanden na de voltooiing van de controle;
 - ii. in de periode van tien jaar vóór aanvang van de controle geen controlediensten uit hoofde van dit artikel hebben verleend aan de betrokken aanbieder van cloudcomputingdiensten of aan een met die aanbieder verbonden rechtspersoon;
 - iii. de controle niet uitvoeren tegen vergoedingen die afhankelijk zijn van het resultaat van de controle;
 - b) beschikken over aantoonbare deskundigheid, technische bekwaamheid en capaciteiten op het gebied van controles van cloudcomputingdiensten;

- c) blijken hebben gegeven van objectiviteit en beroepsethiek, met name op basis van het naleven van codes voor goede praktijken of gepaste normen.
5. De controleorganisaties die de controles uitvoeren, stellen voor elke controle een controlerapport op. Dat verslag wordt schriftelijk gemotiveerd en bevat ten minste het volgende:
- a) de naam, het adres en de contactpersoon van de aan de controle onderworpen aanbieder, en de bestreken periode;
 - b) de naam en het adres van de controleorganisatie(s) die de controle uitvoert (uitvoeren);
 - c) een belangenverklaring;
 - d) een beschrijving van de specifieke gecontroleerde aspecten en de toegepaste methode;
 - e) een beschrijving en een samenvatting van de belangrijkste bevindingen van de controle;
 - f) een lijst van de derden die in het kader van de controle zijn geraadpleegd;
 - g) een “positief” of “negatief” controleadvies en alle informatie over de vraag of de gecontroleerde dienst van de gecontroleerde aanbieder voldoet aan de toepasselijke controlecriteria voor Uniebetrouwbaarheidsniveau 2, 3 of 4 overeenkomstig bijlage II;
 - h) indien het controleadvies “negatief” is, operationele aanbevelingen over specifieke maatregelen om naleving te bereiken, alsmede het aanbevolen tijdsbestek om naleving te bereiken;
 - i) indien het controleadvies “positief” is, het Uniebetrouwbaarheidsniveau dat moet worden erkend op grond van artikel 17, afgegeven aan de gecontroleerde dienst van de gecontroleerde aanbieder overeenkomstig de toepasselijke criteria van bijlage II.
6. Wanneer de controleorganisatie niet in staat was bepaalde specifieke aspecten te controleren of op basis van haar onderzoeken een controleadvies te geven, bevat het controlerapport een toelichting op de omstandigheden en de redenen die ertoe leidden dat die aspecten niet konden worden gecontroleerd.
7. De controleorganisatie kan haar controlerapport en controleadvies intrekken indien de gecontroleerde aanbieder opzettelijk of uit onachtzaamheid onjuiste of misleidende controlebewijs heeft verstrekt.
8. De gecontroleerde aanbieder dient het controlerapport en het bijbehorende “positieve” controleadvies jaarlijks ter beoordeling in bij dezelfde of een andere controleorganisatie, die beoordeelt of de gecontroleerde dienst nog steeds voldoet aan de toepasselijke criteria van bijlage II. Op basis van de jaarlijkse beoordeling kan de controleorganisatie het oorspronkelijke controlerapport en het oorspronkelijke controleadvies bevestigen, bijwerken of intrekken.
9. De Commissie is bevoegd overeenkomstig artikel 45 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen met regels voor de uitvoering van controles van de procedurele stappen, regels voor controleorganisaties en hun technische competenties, controlemethoden en modellen voor de controlerapporten.

Artikel 21

Inhoud en kwaliteit van het controlebewijs

1. Om het controlerapport en het controleadvies op te stellen, beoordeelt de controleorganisatie of de gecontroleerde dienst voldoet aan de criteria van bijlage II op basis van het in bijlage III vermelde controlebewijs. De Commissie is bevoegd overeenkomstig artikel 45 gedelegeerde handelingen vast te stellen om bijlage III te wijzigen door de nodige bewijsstukken vast te stellen om de controlecriteria van bijlage II te beoordelen.
2. Het controlebewijs moet:
 - a) relevant en toereikend zijn om de controleorganisatie in staat te stellen een controlerapport op te stellen en een controleadvies te geven, en
 - b) naar het professioneel oordeel en overeenkomstig de professioneel-kritische instelling van de controleorganisatie, betrouwbaar zijn.

Artikel 22

Centraal register van cloudcomputingdiensten

1. De Commissie zorgt voor het opzetten en bijhouden van een specifiek register van cloudcomputingdiensten die overeenkomstig artikel 17 zijn erkend (“centraal register”).
2. De nationale bevoegde autoriteit van vestiging die een cloudcomputingdienst overeenkomstig artikel 17 heeft erkend, registreert de cloudcomputingdienst in het centrale register.
3. De intrekking van een controlerapport en een controleadvies door een controleorganisatie of de intrekking van een erkenning door een bevoegde autoriteit wordt bekendgemaakt in het centrale register en blijft daar vijf jaar beschikbaar.
4. Het centrale register wordt openbaar gemaakt en regelmatig bijgewerkt door de Commissie en de nationale bevoegde autoriteiten van vestiging op een speciale en gemakkelijk toegankelijke website.

Artikel 23

Transparantieverplichtingen

1. Zodra de erkende aanbieder van cloudcomputingdiensten kennis krijgt van informatie of een materiële wijziging in de omstandigheden die van invloed kan zijn op het controlerapport en het “positieve” advies uit hoofde van artikel 20 of de erkenning uit hoofde van artikel 17, stelt hij de controleorganisatie en de nationale bevoegde autoriteit van vestiging daarvan zo spoedig mogelijk in kennis.
2. Op basis van de in lid 1 bedoelde kennisgeving beoordeelt de controleorganisatie of het controlerapport of het controleadvies moet worden gewijzigd of ingetrokken. Indien de controleorganisatie het controlerapport of het controleadvies wijzigt of intrekt, stelt zij de nationale bevoegde autoriteit van vestiging daarvan zo spoedig mogelijk in kennis.
3. Op basis van de in lid 1 of lid 2 bedoelde kennisgeving beoordeelt de nationale bevoegde autoriteit van vestiging of de erkenning moet worden gewijzigd of ingetrokken. Wanneer de nationale bevoegde autoriteit van vestiging de erkenning van de cloudcomputingdienst wijzigt of intrekt, stelt zij de nationale bevoegde

autoriteiten van de andere lidstaten en de Commissie daarvan zo spoedig mogelijk in kennis.

Artikel 24

Sancties en schadevergoeding

1. De lidstaten stellen binnen hun bevoegdheden voorschriften vast betreffende sancties voor inbreuken op dit hoofdstuk door aanbieders van cloudcomputingdiensten en treffen alle nodige maatregelen om ervoor te zorgen dat die sancties worden toegepast. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. De lidstaten stellen de Commissie zo snel mogelijk van die voorschriften en maatregelen in kennis en delen de Commissie alle latere wijzigingen daarvan mee.
2. De lidstaten houden rekening met de volgende niet-uitputtende criteria voor het opleggen van sancties voor inbreuken op deze verordening:
 - a) de aard, de ernst, de omvang en de duur van de inbreuk;
 - b) door de inbreukmakende partij ondernomen actie om de schade als gevolg van de inbreuk te beperken of te herstellen;
 - c) eerdere inbreuken van de inbreukmakende partij;
 - d) de door de inbreukmakende partij verkregen financiële voordelen of vermeden verliezen als gevolg van de inbreuk, voor zover deze voordelen of verliezen op betrouwbare wijze kunnen worden vastgesteld;
 - e) andere verzwarende of verzachtende factoren die van toepassing zijn op de omstandigheden van de zaak;
 - f) de jaaromzet van de inbreukmakende partij in het voorgaande boekjaar in de Unie.
3. Op grond van het Unierecht en het nationale recht hebben afnemers van de cloudcomputingdiensten het recht om aanbieders van cloudcomputingdiensten te verzoeken om schadevergoeding voor alle schade of verliezen geleden als gevolg van een schending door die aanbieders van hun verplichtingen uit hoofde van dit hoofdstuk.

AFDELING 4

NATIONALE BEVOEGDE AUTORITEITEN

Artikel 25

Nationale bevoegde autoriteiten

1. Uiterlijk op [P.O. insert date of entry into force plus 1 year] wijzen de lidstaten één of meer nationale bevoegde autoriteiten aan die verantwoordelijk zijn voor de handhaving van dit hoofdstuk. Daartoe kunnen de lidstaten een bestaande autoriteit of bestaande autoriteiten (“bevoegde autoriteiten”) aanwijzen.
2. De lidstaten stellen de Commissie in kennis van de namen van de bevoegde autoriteiten en van hun taken en bevoegdheden. De Commissie houdt een openbaar register van deze autoriteiten bij.
3. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten hun taken uit hoofde van deze verordening op een onpartijdige, transparante en tijdige wijze uitvoeren. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten over alle nodige middelen

beschikken om hun taken uit te voeren, waaronder toereikende technische, financiële en personele middelen om adequaat toezicht uit te oefenen op alle aanbieders van cloudcomputingdiensten die onder hun bevoegdheid vallen.

4. De lidstaat waar de aanbieder van cloudcomputingdiensten zijn hoofdvestiging heeft, dat wil zeggen waar de aanbieder van cloudcomputingdiensten zijn hoofdkantoor of statutaire zetel heeft van waaruit de belangrijkste financiële functies en operationele controle worden uitgeoefend, is exclusief bevoegd voor de handhaving van dit hoofdstuk.

Artikel 26

Bevoegdheden van de nationale bevoegde autoriteiten

1. Indien dit nodig is om hun taken uit hoofde van artikel 17 uit te voeren, beschikken de bevoegde autoriteiten van vestiging over de volgende onderzoeksbevoegdheden:
 - a) de bevoegdheid om van aanbieders van cloudcomputingdiensten, alsook van andere personen die handelen voor doeleinden die verband houden met hun handel, onderneming, ambacht of beroep, van wie redelijkerwijs kan worden verwacht dat zij op de hoogte zijn van informatie met betrekking tot een vermoedelijke inbreuk op deze verordening, zoals controleorganisaties, te verlangen dat zij die informatie zo spoedig mogelijk verstrekken;
 - b) de bevoegdheid om inspecties uit te voeren, of om een gerechtelijke autoriteit in hun lidstaat te verzoeken inspecties te gelasten, in gebouwen die deze aanbieders of personen die handelen voor doeleinden die verband houden met hun handel, onderneming, ambacht of beroep, gebruiken voor doeleinden die verband houden met hun handel, onderneming, ambacht of beroep, of om andere overheidsinstanties te verzoeken dit te doen, teneinde informatie met betrekking tot een vermeende inbreuk in enige vorm te onderzoeken, in beslag te nemen, te kopiëren of er kopieën van te verkrijgen, ongeacht het opslagmedium;
 - c) de bevoegdheid om personeelsleden of vertegenwoordigers van die aanbieders of personen die handelen voor doeleinden die verband houden met hun handel, onderneming, ambacht of beroep, te verzoeken uitleg te geven over informatie die verband houdt met een vermoedelijke inbreuk en, met hun toestemming, hun antwoorden met ongeacht welk technische middelen ook vast te leggen.
2. Indien dit nodig is om hun taken uit hoofde van artikel 17 uit te voeren, beschikken de nationale bevoegde autoriteiten van vestiging over de volgende handhavingsbevoegdheden:
 - a) de bevoegdheid om de stopzetting van inbreuken te bevelen en, waar passend, remedies op te leggen die in verhouding staan tot de inbreuk en die noodzakelijk zijn om de inbreuk daadwerkelijk te beëindigen, of een gerechtelijke autoriteit in hun lidstaat te verzoeken dit te doen;
 - b) de bevoegdheid om geldboetes op te leggen, of om een gerechtelijke autoriteit in hun lidstaat te verzoeken dit te doen, wegens niet-naleving van deze verordening, waaronder elk van de op grond van lid 1 uitgevaardigde onderzoeksbevel;
 - c) de bevoegdheid om overeenkomstig artikel 24 een dwangsom op te leggen, of een gerechtelijke autoriteit in hun lidstaat te verzoeken dit te doen, om ervoor

te zorgen dat een inbreuk wordt beëindigd in overeenstemming met een krachtens punt a) uitgevaardigd bevel of wegens niet-naleving van de krachtens lid 1 uitgevaardigde onderzoeksbevelen.

3. De maatregelen die de nationale bevoegde autoriteiten van vestiging hebben genomen bij de uitoefening van hun bevoegdheden zoals vermeld in de leden 1 en 2, zijn doeltreffend, ontradend en evenredig, met name rekening houdend met de aard, de ernst, de herhaling en de duur van de inbreuk of vermeende inbreuk waarop deze maatregelen betrekking hebben, alsook, in voorkomend geval, met de economische, technische en operationele capaciteit van de betrokken aanbieder van diensten.
4. De lidstaten stellen specifieke regels en procedures vast voor de uitoefening van de bevoegdheden uit hoofde van de leden 1 en 2 en zorgen ervoor dat elke uitoefening van die bevoegdheden onderworpen is aan passende waarborgen uit hoofde van het toepasselijke nationale recht, met inachtneming van de algemene beginselen van het Unierecht. Deze maatregelen worden met name alleen genomen overeenkomstig het recht op eerbiediging van het privéleven en de rechten van verdediging, waaronder het recht om te worden gehoord en het recht op toegang tot het dossier, en zijn onderworpen aan een doeltreffende voorziening in rechte van alle betrokkenen.

AFDELING 5

WEDERZIJDSE BIJSTAND EN SAMENWERKING

Artikel 27

Wederzijdse bijstand

1. De bevoegde autoriteiten en de Commissie werken nauw samen en verlenen elkaar wederzijdse bijstand om dit hoofdstuk op consistente en efficiënte wijze toe te passen. De wederzijdse bijstand omvat de uitwisseling van informatie.
2. Een bevoegde autoriteit kan andere bevoegde autoriteiten verzoeken specifieke informatie te verstrekken waarover zij beschikken met betrekking tot een specifieke aanbieder van cloudcomputingdiensten om haar onderzoeksbevoegdheden uit hoofde van artikel 26 uit te oefenen met betrekking tot specifieke informatie die zich in hun lidstaat bevindt. Waar passend kan de bevoegde autoriteit die het verzoek ontvangt daarbij andere bevoegde autoriteiten of andere overheidsinstellingen van de betrokken lidstaat betrekken.
3. De bevoegde autoriteit die het verzoek overeenkomstig lid 2 ontvangt, voldoet aan dat verzoek en stelt de bevoegde autoriteit van vestiging zo spoedig mogelijk en uiterlijk twee maanden na ontvangst van het verzoek in kennis van de genomen maatregelen, tenzij naar behoren gemotiveerd.

Artikel 28

Landsgrensoverschrijdende samenwerking

1. Wanneer een bevoegde autoriteit van bestemming redenen heeft om te vermoeden dat een aanbieder van cloudcomputingdiensten niet langer aan de eis van bijlage II bij deze verordening voldoet, kan zij de bevoegde autoriteit van vestiging verzoeken de zaak te beoordelen en de nodige onderzoeks- en handhavingsmaatregelen te treffen om naleving te waarborgen.

2. De Commissie kan de in artikel 25 bedoelde bevoegde autoriteit ook verzoeken de zaak te beoordelen en de nodige onderzoeks- en handhavingsmaatregelen te treffen om naleving te waarborgen.
3. verzoeken op grond van lid 1 of lid 2 worden naar behoren gemotiveerd en worden door de bevoegde autoriteit van vestiging naar behoren in aanmerking genomen. Indien de bevoegde autoriteit van vestiging van oordeel is dat de verstrekte informatie ontoereikend is, kan zij om aanvullende informatie verzoeken. De in lid 4 vastgestelde termijn wordt opgeschort totdat die aanvullende informatie is verstrekt.
4. De bevoegde autoriteit van de plaats van vestiging deelt, zo snel mogelijk en in elk geval niet later dan twee maanden na ontvangst van het verzoek krachtens lid 1 of 2, de beoordeling van de vermeende inbreuk mee aan de bevoegde autoriteit die het verzoek heeft verzonden en aan de Commissie, samen met een toelichting van eventuele onderzoeks- of handhavingsmaatregelen die in verband daarmee zijn genomen of overwogen om de naleving van deze verordening te waarborgen.

Hoofdstuk II

Maatregelen aan de vraagzijde

AFDELING 1

OVERHEIDSOPDRACHTEN

Artikel 29

Risicobeoordelingen

1. Uiterlijk op [date of entry into force plus 1 year], en vervolgens om de twee jaar, of telkens wanneer dat nodig is, voeren de lidstaten en de entiteiten van de Unie risicobeoordelingen uit die:
 - a) de openbare diensten identificeren die gebruikmaken of zullen gebruikmaken van cloudcomputingdiensten die bijdragen tot de handhaving van de openbare orde in sectoren die onder bijlage I of II bij Richtlijn (EU) 2022/2555 vallen en op het gebied van nationale veiligheid, interne veiligheid, beheer van de buitengrenzen, defensie, justitie of rechtshandhaving, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten;
 - b) bepalen welk in bijlage II bij deze verordening vermeld Uniebetrouwbaarheidsniveau 2, 3 of 4 geschikt is voor de geïdentificeerde openbare diensten.

Wanneer de entiteiten van de Unie en de lidstaten verantwoordelijkheden met betrekking tot de openbare diensten delen, overwegen zij, in voorkomend geval, de desbetreffende risicobeoordeling(en) gezamenlijk uit te voeren.
2. Bij de uitvoering van hun risicobeoordelingen houden de lidstaten en de entiteiten van de Unie ten minste rekening met de volgende aspecten:
 - a) de gevoeligheid, het kritieke karakter en de omvang van de verwerkte niet-persoonsgebonden gegevens, inclusief de mogelijke gevolgen voor de openbare orde en de aard, de omvang, de context en het doel van de verwerking van persoonsgegevens, alsook het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van betrokkenen;

- b) het risico en de daaruit voortvloeiende gevolgen voor de openbare orde van onrechtmatige toegang uit hoofde van het Unierecht tot dergelijke gegevens door een derde land of een in een derde land gevestigde juridische entiteit;
 - c) het risico en de daaruit voortvloeiende gevolgen voor de openbare orde van een mogelijke verstoring van de dienstverlening.
3. De Commissie specificeert door middel van uitvoeringshandelingen overeenkomstig artikel 46, lid 2, de toe te passen methode, de te gebruiken modellen en de elementen waarmee de lidstaten en de entiteiten van de Unie rekening moeten houden bij het uitvoeren van de in lid 1 bedoelde risicobeoordelingen. In de methode wordt gespecificeerd hoe de lidstaten het hoogste zekerheidsniveau gebruiken voor de meest kritieke openbare diensten, waaronder maar niet beperkt tot, defensie.
 4. Binnen drie maanden na de uitvoering van de in lid 1 bedoelde risicobeoordelingen verstrekken de lidstaten de Commissie de resultaten van die risicobeoordelingen, waarbij zij aangeven wanneer zij afwijken van de in lid 3 bedoelde uitvoeringshandelingen.
 5. Indien de Commissie na evaluatie van de resultaten van de risicobeoordeling(en) van een lidstaat tot de conclusie komt dat het Uniebetrouwbaarheidsniveau dat in een risicobeoordeling voor de openbare dienst is vastgesteld, niet passend is of de punten van zorg met betrekking tot de openbare orde niet adequaat aanpakt, kan de Commissie overeenkomstig artikel 46, lid 2, uitvoeringshandelingen vaststellen waarin de Uniebetrouwbaarheidsniveaus worden gespecificeerd die nodig zijn voor de openbare dienst.
 6. Wanneer de risicobeoordeling de migratie naar een andere cloudcomputingdienst vereist, migreert de lidstaat of entiteit van de Unie binnen een redelijke overgangsperiode van maximaal 12 maanden, rekening houdend met de technische haalbaarheid, de continuïteit van de dienst en de vereisten inzake gegevensoverdraagbaarheid die op die migratie van toepassing zijn.
 7. De lidstaten werken met elkaar en met de Commissie samen via gevestigde coherentiemechanismen en bevorderen de samenwerking en de doeltreffende uitwisseling van informatie en beste praktijken.
 8. Voor de toepassing van lid 3 is de Commissie bevoegd aanbieders van cloudcomputingdiensten te verzoeken alle nodige informatie te verstrekken.
 9. In hun risicobeoordelingen overwegen de lidstaten en de entiteiten van de Unie of een strategie met meerdere aanbieders of meerdere clouds passend is als onderdeel van hun aanbesteding van cloudcomputingdiensten.

Artikel 30

Overheidsopdrachten

1. Dit artikel is van toepassing op aanbestedende diensten die cloudcomputingdiensten inkopen voor exclusief gebruik. Onverminderd artikel 136 van Verordening (EU, Euratom) 2024/2509 is dit artikel ook van toepassing op entiteiten van de Unie die cloudcomputingdiensten inkopen voor exclusief gebruik.
2. Entiteiten van de Unie en openbare lichamen waarvan in het kader van de in artikel 29, lid 1, bedoelde risicobeoordeling niet is vastgesteld dat hun openbare diensten bijdragen tot de handhaving van de openbare orde, maken gebruik van

cloudcomputingdiensten die overeenkomstig artikel 17 zijn erkend als diensten met Uniebetrouwbaarheidsniveau 1.

3. Aanbestedende diensten, waaronder de namens hen optredende entiteiten, waarvan is vastgesteld dat hun activiteiten bijdragen tot de handhaving van de openbare orde uit hoofde van artikel 29, lid 1, in sectoren die onder bijlage I of II bij Richtlijn (EU) 2022/2555 vallen en op het gebied van nationale veiligheid, interne veiligheid, beheer van de buitengrenzen, defensie, justitie of rechtshandhaving, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, kopen alleen cloudcomputingdiensten in waarvan is erkend dat zij Uniebetrouwbaarheidsniveau 2, 3 of 4 hebben.
4. In afwijking van de leden 2 of 3 kunnen aanbestedende diensten bij wijze van uitzondering en indien naar behoren gemotiveerd, besluiten geen cloudcomputingdiensten aan te besteden waarvan is erkend dat zij Uniebetrouwbaarheidsniveau 1, 2, 3 of 4 hebben, indien één of meer van de volgende omstandigheden van toepassing zijn:
 - a) het voorwerp van de inschrijving kan niet worden geleverd door erkende cloudcomputingdiensten die in het in artikel 22 bedoelde centrale register staan vermeld, en er bestaat geen geschikt of redelijk alternatief of vergelijkbare cloudcomputingdienst, en het ontbreken van een dergelijke dienst is niet het gevolg van een kunstmatige beperking van de parameters van de aanbestedingsprocedure;
 - b) de aanbestedende dienst heeft in het voorgaande jaar een soortgelijke aanbestedingsprocedure gestart, maar geen geschikte inschrijvingen ontvangen of er hebben zich geen geschikte deelnemers gemeld;
 - a) de toepassing van de vereisten van deze verordening zou de aanbestedende dienst ertoe verplichten diensten tegen onevenredige kosten aan te besteden.

AFDELING 2

ENTITEITEN IN DE PARTICULIERE SECTOR

Artikel 31

Effectbeoordelingen

1. De in bijlage I bij Richtlijn (EU) 2022/2555 bedoelde entiteiten die geen openbare lichamen zijn, kunnen soortgelijke beoordelingen uitvoeren als die welke in artikel 29 zijn vermeld.
2. De Commissie kan richtsnoeren uitvaardigen over de methode voor het uitvoeren van de effectbeoordelingen uit hoofde van dit artikel en over mogelijke risicobeperkende maatregelen die moeten worden genomen door entiteiten uit de particuliere sector die actief zijn in zeer kritieke sectoren.
3. Indien de Commissie wegens specifieke omstandigheden en in naar behoren gemotiveerde gevallen en in overleg met de lidstaten tot de conclusie komt dat entiteiten die geen openbare lichamen zijn en die actief zijn in zeer kritieke sectoren, een effectbeoordeling nodig hebben, kan de Commissie overeenkomstig artikel 45 ter aanvulling van deze verordening gedelegeerde handelingen vaststellen waarin de noodzaak van een dergelijke effectbeoordeling en de risicobeperkende maatregelen die die entiteiten die geen openbare lichamen zijn, moeten nemen, worden gespecificeerd.

AFDELING 3

ANDERE MAATREGELEN IN VERBAND MET AANBESTEDINGEN

Artikel 32

Meerwaarde voor de Unie

1. In openbare aanbestedingsprocedures voor innovatieve cloudcomputingdiensten en AI-systemen nemen aanbestedende diensten, als onderdeel van de kwaliteitsbeoordeling van de inschrijving, niet-prijsgerelateerde gunningscriteria op aan de hand waarvan zij de bijdrage van de inschrijver aan de ontwikkeling van een Europees cloud- en AI-ecosysteem kunnen beoordelen.
2. Bij de toepassing van niet-prijsgerelateerde gunningscriteria uit hoofde van lid 1 zorgen de aanbestedende diensten ervoor dat de niet-prijsgerelateerde gunningscriteria:
 - a) gerelateerd zijn aan het voorwerp van de opdracht;
 - b) de aanbestedende dienst geen onbeperkte keuzevrijheid verlenen;
 - c) uitdrukkelijk worden vermeld in de aanbestedingsdocumenten of in het aanbestedingsbericht;
 - d) bijkomstig en niet doorslaggevend zijn bij de gunning van de opdracht.
3. Zonder afbreuk te doen aan de discretionaire bevoegdheid van de aanbestedende diensten om aanvullende criteria toe te passen, stellen de in lid 1 bedoelde niet-prijsgerelateerde gunningscriteria de aanbestedende diensten in staat te beoordelen in hoeverre:
 - a) de inschrijver bijdraagt tot de versterking van de toeleveringsketen voor digitale technologie in de Unie, inclusief het gebruik van software of hardware die in de Unie is ontworpen of vervaardigd;
 - b) de inschrijver in de Unie ontwikkelde technologieën heeft geïntegreerd, inclusief de resultaten van onderzoek en ontwikkeling die voortvloeien uit door de Unie gefinancierde onderzoeks- en ontwikkelingsprogramma's, en gebruikmaakt van instrumenten zoals normen, specificaties, software, modellen of andere in de Unie ontwikkelde technologieën;
 - c) de innovatie die nodig is om de dienst te verlenen, bijdraagt tot de versterking van de voorzieningszekerheid en de ontwikkeling van een Europees cloud- en AI-ecosysteem;
 - d) de dienst, voor zover dit haalbaar is met betrekking tot de beschikbaarheid op de markt en de technische vereisten, wordt verleend via kritieke hardwarecomponenten voor computers, opslag en netwerken die in de Unie zijn ontworpen en/of vervaardigd, of, indien dit niet haalbaar is, via hardwarecomponenten uit een derde land die bijdragen tot de versterking van de voorzieningszekerheid en de ontwikkeling van een Europees cloud- en AI-ecosysteem.

Artikel 33

Monitoring van aanbesteding voor innovatie op het gebied van cloud en AI

1. De lidstaten monitoren en brengen verslag uit over hun gebruik van aanbestedingsprocedures voor innovatie op het gebied van cloudcomputingdiensten en AI-systemen.
2. De lidstaten nemen passende maatregelen om ervoor te zorgen dat de in lid 1 bedoelde monitoring en verslaglegging actief worden gebruikt om belemmeringen voor de deelname van kmo's aan aanbestedingsprocedures in kaart te brengen, de toegang van kmo's tot aanbestedingsmarkten te verbeteren, het ontwerp van vereenvoudigde, evenredige en kmo-vriendelijke aanbestedingsstrategieën te ondersteunen, zoals splitsing in percelen, waar passend, de deelname van kmo's aan de innovatieprocedure van Richtlijn 2014/24/EU en precommerciële inkoop van cloudcomputingdiensten en AI-systemen te bevorderen.
3. Op basis van de in lid 1 bedoelde monitoring stellen de lidstaten de Commissie jaarlijks in kennis van de volgende informatie:
 - a) de omvang van de ondernemers die aan dergelijke aanbestedingen deelnemen;
 - b) trends in de deelname van kmo's, zoals het aantal aan kmo's gegunde opdrachten, hun aandeel in de totale waarde van de opdracht, als percentage, en, indien beschikbaar, het aandeel van landsgrensoverschrijdende deelname van kmo's;
 - c) maatregelen die zijn genomen om de toegang van kmo's tot openbare aanbestedingsprocedures te verbeteren.
4. De lidstaten streven ernaar dat ten minste 25 % van hun aanbestedingen voor cloudcomputingdiensten en AI-systemen wordt gegund aan innovatieve kmo's. De lidstaten nemen in hun in artikel 7 bedoelde nationale strategieën plannen op over de wijze waarop zij voornemens zijn deze doelstelling te verwezenlijken.
5. Entiteiten van de Unie en aanbestedende diensten bevorderen:
 - a) voorafgaande marktraadplegingen;
 - b) matchmaking tussen overheidsafnemers en innovatieve oplossingen van Europese kmo's en start-ups;
 - c) de ontwikkeling van contractuele bepalingen voor overheidsopdrachten die gunstig zijn voor innovatieve kmo's.

Hoofdstuk III

Europese cloudfederatie voor de publieke sector

Artikel 34

Oprichting van de Europese cloudfederatie voor de publieke sector

1. Hierbij wordt de Europese cloudfederatie voor de publieke sector ("Federatie EuroCloud") opgericht. De Federatie EuroCloud staat open voor deelname op vrijwillige basis van entiteiten van de Unie en openbare lichamen. Entiteiten van de Unie en openbare lichamen kunnen bij de Commissie een verzoek indienen om zich bij de Federatie EuroCloud aan te mogen sluiten.

2. De Federatie EuroCloud faciliteert het delen van datacentrumdiensten en cloudcomputingdiensten tussen entiteiten van de Unie en openbare lichamen onder de voorwaarden van de artikelen 35 en 36.
3. De Commissie richt een platform op voor de Federatie EuroCloud dat ten minste voorziet in:
 - a) een catalogus met informatie over beschikbare datacentrumdiensten en cloudcomputingdiensten voor de overheidssector;
 - b) een dienstenplatform voor de uitwisseling en orkestratie van computer-, opslag- en netwerkmiddelen en -diensten.
4. De Commissie is bevoegd uitvoeringshandelingen vast te stellen om de procedure voor deelname aan de Federatie EuroCloud en het model voor de inhoud en andere details van het verzoek om deelname te specificeren. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 35

Delen van datacentrumdiensten en cloudcomputingdiensten voor de overheidssector

1. Een lid van de Federatie EuroCloud (de “delende entiteit”) kan datacentrumdiensten en cloudcomputingdiensten delen met een ander lid van de Federatie EuroCloud (de “gebruikende entiteit”) indien de delende entiteit direct, of indirect via een intermediaire juridische entiteit, eigenaar is van de hardware waarlangs de dienst beschikbaar wordt gesteld en de dienst verleent die beschikbaar wordt gesteld aan de gebruikende entiteit. Indien de delende entiteit indirect eigenaar is van de hardware en de diensten verleent via een intermediaire juridische entiteit, oefent de delende entiteit zeggenschap uit over die intermediaire juridische entiteit.
2. De delende entiteit neemt passende technische, operationele en organisatorische maatregelen om een doeltreffende, veilige en veerkrachtige dienstverlening te waarborgen.
3. Alvorens datacentrumdiensten en cloudcomputingdiensten binnen de Federatie EuroCloud te delen, toont de delende entiteit aan de Commissie aan dat zij voldoet aan de voorwaarden van de leden 1 en 2.
4. De Commissie beoordeelt de door de delende entiteit verstrekte informatie en staat de delende entiteit toe datacentrumdiensten en cloudcomputingdiensten binnen de Federatie EuroCloud te delen indien aan de voorwaarden van de leden 1 en 2 is voldaan.
5. De delende entiteit kan de gebruikende entiteit een vergoeding in rekening brengen. Het bedrag van de vergoeding is beperkt tot de kosten die de delende entiteit maakt in verband met het delen van de dienst en vormt geen bezwarende titel in de zin van artikel 2 van Richtlijn 2014/24/EU en Verordening (EU, Euratom) 2024/2509.
6. De Commissie is bevoegd uitvoeringshandelingen vast te stellen om de in lid 2 bedoelde technische, operationele en organisatorische maatregelen te specificeren. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 36

Vergoedingen voor het beheer van de Federatie EuroCloud

1. De kosten die voortvloeien uit de activiteiten die de Commissie overeenkomstig dit hoofdstuk uitvoert, worden gezamenlijk gefinancierd door de leden van de Federatie EuroCloud door middel van vergoedingen die door de Commissie in rekening worden gebracht.
2. Indien de kosten in eerste instantie ten laste komen van de algemene begroting van de Unie, worden zij door de EuroCloud-leden terugbetaald over een periode van ten hoogste drie jaar vanaf de datum waarop de kosten door de Unie zijn gedragen.
3. Ontvangsten in de vorm van vergoedingen vormen interne bestemmingsontvangsten in de zin van artikel 21, lid 3, punt a), van Verordening (EU, Euratom) 2024/2509. Deze inkomsten worden gebruikt om de kosten te dekken van de activiteiten die de Commissie overeenkomstig dit hoofdstuk uitvoert, waaronder de beoordeling van het verzoek om toe te treden tot de Federatie EuroCloud en de oprichting van het in artikel 34, lid 3, bedoelde platform. Resterende ontvangsten na aftrek van die kosten worden opgenomen in de begroting van de Unie.
4. De Commissie stelt uitvoeringshandelingen met gedetailleerde regels vast voor het bepalen van de geschatte kosten, het afzonderlijke bedrag van de vergoedingen en de wijze waarop en omstandigheden waaronder deze moeten worden betaald. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Hoofdstuk IV

Aanbesteding van datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen door de Commissie

Artikel 37

Aanbestedingsactiviteiten van de Commissie

1. De Commissie kan aanbestedingsactiviteiten uitvoeren voor de inkoop van datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen voor zichzelf en voor entiteiten van de Unie en voor aanbestedende diensten van de lidstaten, in overeenstemming met Verordening (EU, Euratom) 2024/2509, met inachtneming van de in dit hoofdstuk vastgestelde uitzonderingen. In afwijking van artikel 168 van Verordening (EU, Euratom) 2024/2509 kunnen door de Commissie geselecteerde partnerorganisaties als bedoeld in artikel 168, lid 3, van die verordening ook deelnemen aan de in dit hoofdstuk beschreven aanbestedingsactiviteiten. Aanbestedende diensten van lidstaten, entiteiten van de Unie en door de Commissie geselecteerde partnerorganisaties worden beschouwd als “deelnemende entiteiten” in de zin van dit hoofdstuk.
2. Aanbestedende diensten kunnen in eigen naam of als aankoopcentrale in de zin van artikel 2, lid 1, punt 16), van Richtlijn 2014/24/EU aan de aanbestedingsprocedures deelnemen wanneer zij als zodanig worden aangemerkt. Er kunnen specifieke regels en verplichtingen betreffende hun deelname worden opgelegd wanneer zij als aankoopcentrale deelnemen aan de in artikel 38 bedoelde overeenkomst.
3. Naast de aanbestedingsactiviteiten waarin artikel 168 van Verordening (EU, Euratom) 2024/2509 voorziet, kan de Commissie optreden als aankoopcentrale voor

aanbestedende diensten van de lidstaten en door de Commissie geselecteerde partnerorganisaties, door:

- a) datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen in te kopen namens of voor rekening van een of meer aanbestedende diensten van de lidstaten en door de Commissie geselecteerde partnerorganisaties, door het sluiten van raamovereenkomsten of het exploiteren van dynamische inkoopssystemen voor diensten die bestemd zijn voor de deelnemende entiteiten;
 - b) op te treden als groothandelaar door deze diensten te verwerven en te leveren en door te verkopen of, in uitzonderlijke omstandigheden, te schenken aan een of meer aanbestedende diensten van de lidstaten.
4. Bij de uitvoering van aanbestedingsactiviteiten kan de Commissie aanvullende steun verlenen aan deelnemende entiteiten, waaronder:
- a) de technische infrastructuur die de deelnemende entiteiten in staat stelt gegunde opdrachten te gebruiken of opdrachten te gunnen, waaronder specifieke opdrachten in het kader van gesloten raamovereenkomsten, voor datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen;
 - b) advies en ondersteuning bij de voorbereiding en uitvoering van aanbestedingsprocedures;
 - c) voorbereiding en uitvoering van aanbestedingsprocedures namens of voor rekening van de betrokken entiteiten;
 - d) facturering en andere administratieve diensten in verband met de gegunde opdrachten.
5. Dergelijke aanvullende steun kan rechtstreeks door de Commissie worden verleend, via een onderaannemer of door delegatie aan organen of agentschappen van de Unie. De toetreding van deelnemende entiteiten tot de in artikel 38 bedoelde overeenkomst kan afhankelijk worden gesteld van de aanvaarding van een of meer ondersteunende diensten.
6. De Commissie kan een gemeenschappelijk aanbestedingsplatform opzetten en beheren, waaronder diensten die kunnen worden gebruikt om de aanbestedingsactiviteiten in het kader van dit hoofdstuk te vergemakkelijken.

Artikel 38

Regelingen voor de aanbestedingsactiviteiten van de Commissie

1. Alvorens een aanbestedingsactiviteit uit hoofde van artikel 37 uit te voeren, sluiten de Commissie en ten minste twee lidstaten een overeenkomst waarin de praktische regelingen worden vastgelegd voor de aanbestedingsactiviteiten die de Commissie uit hoofde van dit hoofdstuk uitvoert. De overeenkomst heeft betrekking op aanbestedingsprocedures die tijdens de geldigheidsduur ervan moeten worden uitgevoerd en wordt geacht te voldoen aan de vereisten van de gezamenlijke aanbestedingsovereenkomst en het mandaat als bedoeld in artikel 168, leden 2 en 3, van Verordening (EU, Euratom) 2024/2509.
2. De overeenkomst vormt een mandaat voor de Commissie om namens of in naam van de deelnemende entiteiten in de zin van artikel 168, lid 3, punt e), van Verordening (EU, Euratom) 2024/2509 aanbestedingen uit te schrijven.

3. De overeenkomst bevat de praktische regelingen voor de deelname van entiteiten, het besluitvormingsproces voor de keuze van de procedure en de toepasselijke voorwaarden, de beoordeling van verzoeken tot deelname en inschrijvingen, de gunning van opdrachten, en het toepasselijke recht en de bevoegde rechterlijke instantie. De Commissie blijft verantwoordelijk voor de uitvoering en het beheer van aanbestedingsactiviteiten, waaronder besluiten over de aanvang van een aanbestedingsprocedure, het soort procedure en opdracht, en de gunning van opdrachten.
4. Bij de overeenkomst wordt een stuurgroep opgericht, bestaande uit de Commissie en één vertegenwoordiger van elke deelnemende lidstaat op nationaal niveau. De lidstaten kunnen in een later stadium tot de overeenkomst toetreden en worden vervolgens in de stuurgroep vertegenwoordigd. De stuurgroep kan extra vertegenwoordigers van andere entiteiten van de Unie, van aanbestedende diensten van de lidstaten en van door de Commissie geselecteerde partnerorganisaties benoemen.
5. De stuurgroep is verantwoordelijk voor het strategische toezicht op de aanbestedingsactiviteiten, onder meer voor het voorstellen van de strategische richting van de aanbestedingsagenda voor een vastgestelde periode, en voor het goedkeuren van de strategische richting van elke aanbestedingsprocedure voordat deze door de Commissie wordt gestart, om ervoor te zorgen dat deze in overeenstemming is met het bij deze verordening vastgestelde kader.
6. Zodra de overeenkomst in werking is getreden, kunnen aanbestedende diensten van deelnemende lidstaten, entiteiten van de Unie en door de Commissie geselecteerde partnerorganisaties toetreden tot en profiteren van de overeenkomst, en worden zij beschouwd als deelnemende entiteiten aan de procedures waaraan zij wensen deel te nemen. De stuurgroep kan bepalen dat de overeenkomst de vorm aanneemt van een toetredingsovereenkomst.
7. De deelname van een aanbestedende dienst van een lidstaat is niet afhankelijk van de deelname van die lidstaat.
8. De stuurgroep stelt transparante en niet-discriminerende voorwaarden vast waaronder aanbestedende diensten van de lidstaten tot de overeenkomst kunnen toetreden, met name wat betreft omvang, minimumbedragen en andere objectieve criteria. De stuurgroep stelt ook de regels en procedures vast voor de beëindiging van de deelname aan de overeenkomst van een aanbestedende dienst van een lidstaat die zijn verplichtingen uit hoofde van de overeenkomst niet is nagekomen.
9. In afwijking van artikel 168, lid 2, van Verordening (EU, Euratom) 2014/2509 kan de stuurgroep de deelname van aanbestedende diensten uit EVA-staten en kandidaat-lidstaten van de Unie goedkeuren zonder dat een bilateraal of multilateraal verdrag in die mogelijkheid voorziet.
10. De stuurgroep kan de toetreding tot de overeenkomst afhankelijk stellen van de aanvaarding door de deelnemende entiteiten van een of meer ondersteunende diensten als bedoeld in artikel 37.
11. De stuurgroep stelt op voorstel van de Commissie zijn reglement van orde vast.

Artikel 39

Toepasselijk kader voor overheidsopdrachten

1. Een deelnemende entiteit wordt geacht aan haar verplichtingen uit hoofde van het toepasselijke Unierecht inzake overheidsopdrachten te hebben voldaan wanneer zij leveringen of diensten verwerft door middel van opdrachten die door de Commissie op grond van dit hoofdstuk worden gegund, onder meer door middel van raamovereenkomsten die worden gesloten door of dynamische aankoopssystemen die worden beheerd door de Commissie die hierbij optreedt als aankoopcentrale, of aanvullende ondersteunende diensten als bedoeld in artikel 37.
2. De voor de instellingen van de Unie geldende procedurele bepalingen zijn van toepassing op de procedures voor de gunning van specifieke opdrachten in het kader van raamovereenkomsten of dynamische aankoopssystemen.
3. Een aanbestedende dienst die datacentrumdiensten, cloudcomputingdiensten, software en AI-systemen van de Commissie als aankoopcentrale heeft verworven, zorgt er in zijn overeenkomsten met de aanbestedende diensten die hij bedient voor dat alle contractuele vereisten waaraan hij zelf gebonden is, worden nageleefd.
4. De Commissie kan besluiten een aanbestedingsprocedure te starten die openstaat voor deelnemende entiteiten zonder voorafgaand specifiek verzoek van die entiteiten.
5. In afwijking van artikel 168 van Verordening (EU, Euratom) 2024/2509 kunnen deelnemende entiteiten de Commissie gedurende de gehele geldigheidsduur van een dynamisch aankoopstelsel verzoeken om aan het stelsel te mogen deelnemen. Een dergelijk verzoek wordt door de Commissie goedgekeurd op voorwaarde dat de cumulatieve verzoeken niet meer bedragen dan 50 % van de oorspronkelijk geraamde hoeveelheden van de voorgenomen aankopen. De deelname wordt binnen 10 werkdagen na ontvangst van het verzoek goedgekeurd waarmee wordt toegestaan dat de deelnemende entiteiten bij een toekomstige uitnodiging tot inschrijving worden betrokken.
6. De in lid 5 bedoelde mogelijkheid staat alleen open voor deelnemende entiteiten die tot de in artikel 38 bedoelde overeenkomst toetreden nadat het dynamische aankoopstelsel van start is gegaan.

Artikel 40

Vergoedingen voor aanbestedingsactiviteiten

1. De kosten die voortvloeien uit de aanbestedingsactiviteiten die overeenkomstig dit hoofdstuk worden uitgevoerd, worden door de deelnemende entiteiten gezamenlijk gefinancierd door middel van vergoedingen die door de Commissie in rekening worden gebracht.
2. De kosten voor het opzetten van de in artikel 37 bedoelde gemeenschappelijke aanbestedingsactiviteiten, waaronder de ontwikkeling van het gemeenschappelijke aanbestedingsplatform, kunnen in eerste instantie ten laste komen van de algemene begroting van de Unie. In dat geval worden zij door de deelnemende entiteiten terugbetaald over een periode van ten hoogste drie jaar vanaf de datum waarop zij ten laste van de Unie zijn gekomen. De Commissie kan uitvoeringshandelingen vaststellen waarin de praktische en operationele regelingen voor de terugbetaling door de deelnemende entiteiten worden vastgelegd. Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

3. Ontvangsten in de vorm van vergoedingen vormen interne bestemmingsontvangsten in de zin van artikel 21, lid 3, punt a), van Verordening (EU, Euratom) 2024/2509. Deze ontvangsten worden gebruikt om de kosten van de overeenkomstig artikel 37 uitgevoerde aanbestedingsactiviteiten te dekken. Resterende ontvangsten na aftrek van die kosten worden opgenomen in de begroting van de Unie.
4. De vergoedingen worden vooraf vastgesteld, staan in verhouding tot de geraamde kosten van de activiteiten waarvoor vergoedingen in rekening worden gebracht, zoals op kosteneffectieve wijze bepaald, rekening houdend met de praktijken van vergelijkbare aanbestedingskaders, en zijn toereikend om die kosten te dekken.
5. 5. De Commissie stelt uitvoeringshandelingen vast met nadere regels betreffende het bepalen van de vergoedingen, waarbij het volgende wordt gespecificeerd:
 - a) de geraamde kosten die kunnen worden toegerekend aan de aanbestedingsactiviteiten waarvoor vergoedingen in rekening worden gebracht;
 - b) de individuele bedragen van de in rekening te brengen vergoedingen;
 - c) de wijze waarop en de voorwaarden waaronder de vergoedingen moeten worden betaald;
 - d) de voorwaarden waaronder de vergoedingen moeten worden betaald.Die uitvoeringshandelingen worden volgens de in artikel 46, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Hoofdstuk V

Open source

Artikel 41

Bevordering van opensourceoplossingen en het “open source eerst”-beginsel

De Unie en de lidstaten nemen de nodige maatregelen om entiteiten van de Unie en openbare lichamen aan te moedigen bij het bouwen van hun cloud- en AI-ecosysteem of -stack gebruik te maken van open normen en componenten die onder een opensourcelicentie zijn vrijgegeven en het hergebruik ervan te vergemakkelijken, rekening houdend met functionaliteiten, waaronder beveiliging, totale kosten en andere relevante, naar behoren gemotiveerde objectieve criteria.

Artikel 42

Delen en hergebruiken van software

Wanneer entiteiten van de Unie of openbare lichamen software waarop zij intellectuele-eigendomsrechten hebben, beschikbaar stellen voor hergebruik in het kader van een opensourcelicentie, maken zij daartoe gebruik van een catalogus die of register dat gekoppeld is aan en toegankelijk wordt gemaakt via de in artikel 43 bedoelde EU-OSS-catalogus.

Artikel 43

De EU-catalogus van opensourceoplossingen

1. De Commissie verstrekt en onderhoudt een EU-catalogus van opensourceoplossingen (“EU-OSS-catalogus”) als gecentraliseerde catalogus om toegang te krijgen tot software die door entiteiten van de Unie en openbare lichamen beschikbaar wordt gesteld voor hergebruik.

2. De EU-OSS-catalogus wordt gehost op het in artikel 8 van Verordening (EU) 2024/903 genoemde Interoperabel Europa-portaal en is kosteloos elektronisch toegankelijk.
3. De Commissie neemt op basis van objectieve en relevante criteria een besluit over het verzoek van een entiteit van de Unie die of openbaar lichaam dat eigenaar is van een catalogus of register of die een catalogus of register bijhoudt, om die catalogus of dat register te koppelen aan en toegankelijk te maken via de EU-OSS-catalogus.

Artikel 44

Netwerk van opensourceprogrammabureaus

1. De Commissie richt een netwerk van opensourceprogrammabureaus (“OSPO-netwerk”) op om de samenwerking bij de uitvoering van de verplichtingen uit hoofde van dit hoofdstuk te vergemakkelijken.
2. De opensourceprogrammabureaus die door openbare lichamen op lokaal, regionaal of nationaal niveau in een lidstaat en door entiteiten van de Unie zijn opgericht, kunnen de Commissie verzoeken zich bij het OSPO-netwerk aan te mogen sluiten.
3. Het OSPO-netwerk heeft de volgende taken:
 - a) het faciliteren van de uitwisseling van informatie, ervaring en beste praktijken tussen de lidstaten en de Commissie, met name door gemeenschappelijke technische, juridische en organisatorische uitdagingen te bespreken, onder meer in verband met licentieverlening, beveiliging, onderhoud en aankoop van opensourcesoftware;
 - b) het bevorderen van het delen en hergebruiken van opensourcesoftware door openbare lichamen;
 - c) het op vrijwillige en niet-bindende basis bijdragen aan de ontwikkeling van richtsnoeren, modellen of aanbevelingen voor het delen en hergebruiken van opensourcesoftware;
 - d) het samenwerken aan en uitwisselen van opensourceprojecten van gemeenschappelijk belang voor entiteiten van de Unie en openbare lichamen.
4. De Commissie ondersteunt en coördineert het OSPO-netwerk.
5. De Commissie roept ten minste tweemaal per jaar een vergadering van de leden van het OSPO-netwerk bijeen en zit deze voor. De vergaderingen van het OSPO-netwerk kunnen online worden georganiseerd.

TITEL V

SLOTBEPALINGEN

Artikel 44

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.
2. De bevoegdheid om de in artikel 6, lid 4, artikel 16, lid 2, artikel 20, lid 9, artikel 21, lid 1, en artikel 31, lid 3, bedoelde gedelegeerde handelingen vast te stellen, wordt aan de Commissie verleend voor een onbepaalde periode met ingang van [date of entry into force].
3. Het Europees Parlement of de Raad kan de in artikel 6, lid 4, artikel 16, lid 2, artikel 20, lid 9, artikel 21, lid 1, en artikel 31, lid 3, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.
4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.
5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.
6. Een overeenkomstig artikel 6, lid 4, artikel 16, lid 2, artikel 20, lid 9, artikel 21, lid 1, en artikel 31, lid 3, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Deze termijn wordt op initiatief van het Europees Parlement of de Raad met drie maanden verlengd.

Artikel 46

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dit comité is een comité in de zin van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 47

Evaluatie

1. De Commissie evalueert deze verordening uiterlijk op [date of entry into force plus 4 years] en vervolgens om de vijf jaar, en brengt hierover verslag uit aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité.

2. Het in lid 1 bedoelde verslag gaat in voorkomend geval vergezeld van een voorstel tot wijziging van deze verordening.
3. Bij de uitvoering van de in de lid 1 bedoelde evaluatie houdt de Commissie rekening met de standpunten en bevindingen van het Europees Parlement, de Raad, en van andere relevante instanties of bronnen, en besteedt zij specifiek aandacht aan kleine en middelgrote ondernemingen en de positie van nieuwe concurrenten.

Artikel 48

Inwerkingtreding en toepassing

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is van toepassing met ingang van [same day and month as date of entry into force plus 1 year].

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement
De voorzitter

Voor de Raad
De voorzitter

FINANCIEEL EN DIGITAAL MEMORANDUM

1.	KADER VAN HET VOORSTEL/INITIATIEF	3
1,1.	Benaming van het voorstel/initiatief	3
1,2.	Betrokken beleidsterreinen.....	3
1,3.	Doelstellingen	3
1.3.1.	Algemene doelstellingen.....	3
1.3.2.	Specifieke doelstellingen	3
1.3.3.	Verwachte resultaten en gevolgen	3
1.3.4.	Prestatie-indicatoren.....	3
1,4.	Het voorstel/initiatief betreft:	4
1,5.	Motivering van het voorstel/initiatief	4
1.5.1.	Behoeften waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief.....	4
1.5.2.	Toegevoegde waarde van de deelname van de EU (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder “toegevoegde waarde van het optreden van de EU” verstaan de waarde die het optreden van de Unie oplevert boven op de waarde die door een optreden van alleen de lidstaten zou zijn gecreëerd.	4
1.5.3.	Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan	4
1.5.4.	Verenigbaarheid met het meerjarig financieel kader en eventuele synergie met andere passende instrumenten	5
1.5.5.	Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voorerschikking	5
1,6.	Duur en financiële gevolgen van het voorstel/initiatief	6
1,7.	Wijzen van uitvoering van de begroting	6
2.	BEHEERSMAATREGELEN	8
2,1.	Regels inzake het toezicht en de verslagen	8
2,2.	Beheers- en controlesystemen.....	8
2.2.1.	Rechtvaardiging van de voorgestelde wijzen van uitvoering van de begroting, uitvoeringsmechanismen voor financiering, betalingsvoorwaarden en controlestrategie	8
2.2.2.	Informatie over de vastgestelde risico's en het systeem of de systemen voor interne controle die zijn opgezet om die risico's te beperken	8
2.2.3.	Raming en motivering van de kosteneffectiviteit van de controles (verhouding tussen de controlekosten en de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).	8
2,3.	Maatregelen ter voorkoming van fraude en onregelmatigheden.....	9
3.	GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF	10

3.1.	Rubrieken van het meerjarig financieel kader en betrokken begrotingsonderdelen voor uitgaven.....	10
3.2.	Geraamde financiële gevolgen van het voorstel inzake kredieten	12
3.2.1.	Samenvatting van de geraamde gevolgen voor de beleidskredieten.....	12
3.2.1.1.	Kredieten uit goedgekeurde begroting	12
3.2.1.2.	Kredieten uit externe bestemmingsontvangsten.....	17
3.2.2.	Geraamde output, gefinancierd uit beleidskredieten.....	22
3.2.3.	Samenvatting van de geraamde gevolgen voor de administratieve kredieten	24
3.2.3.1.	Kredieten uit goedgekeurde begroting	24
3.2.3.2.	Kredieten uit externe bestemmingsontvangsten.....	24
3.2.3.3.	Totaal kredieten.....	24
3.2.4.	Geraamde personeelsbehoeften.....	25
3.2.4.1.	Gefinancierd uit goedgekeurde begroting.....	25
3.2.4.2.	Gefinancierd uit externe bestemmingsontvangsten	26
3.2.4.3.	Totale personeelsbehoeften.....	26
3.2.5.	Overzicht van het geschatte effect op met digitale technologie samenhangende investeringen	28
3.2.6.	Verenigbaarheid met het huidige meerjarig financieel kader	28
3.2.7.	Bijdragen van derden	28
3.3.	Geraamde gevolgen voor de ontvangsten	29
4.	DIGITALE DIMENSIES.....	29
4.1.	Voorschriften met digitale relevantie	30
4.2.	Gegevens	30
4.3.	Digitale oplossingen.....	31
4.4.	Interoperabiliteitsbeoordeling	31
4.5.	Maatregelen ter ondersteuning van de digitale uitvoering.....	32

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van een kader van maatregelen ter versterking van het Europese cloud- en AI-ecosysteem (verordening cloud- en AI-ontwikkeling)

Korte titel: verordening cloud- en AI-ontwikkeling

(Voor de EER relevante tekst)

1.2. Betrokken beleidsterreinen

Het voorstel heeft betrekking op beleidsterreinen die verband houden met de ontwikkeling van cloudcomputingdiensten, waarbij de nadruk ligt op het waarborgen van een soepele en tijdige overgang naar hoogwaardige, veerkrachtige en toekomstgerichte digitale ecosystemen. Het heeft tot doel de regelgevingsvoorwaarden te scheppen voor een eengemaakte markt voor cloudcomputingdiensten, investeringen in cloudinfrastructuur en onderzoek en ontwikkeling op het gebied van AI te stimuleren en nieuwe vereisten als gevolg van innovatieve technologieën te ondersteunen. Door de bestaande kaders te moderniseren, heeft het initiatief tot doel efficiënte investeringen te vergemakkelijken, duurzame concurrentie te bevorderen en technologische afhankelijkheden te verminderen, en zo het concurrentievermogen en de weerbaarheid van de Europese Unie in het mondiale cloud- en AI-landschap op lange termijn te ondersteunen. Het voorstel heeft ook tot doel hardnekkige belemmeringen voor het landsgrensoverschrijdend aanbieden van cloudcomputingdiensten weg te nemen en de samenhang en voorspelbaarheid van de regelgeving in de lidstaten te verbeteren.

1.3. Doelstellingen

1.3.1. Algemene doelstellingen

De algemene doelstelling van dit initiatief is de werking van de interne markt voor cloudcomputingdiensten te waarborgen en de voorwaarden te scheppen die nodig zijn voor het concurrentievermogen en de strategische autonomie van de Unie.

1.3.2. Specifieke doelstellingen

Specifieke doelstelling nr. 1: meer rekencapaciteit uitrollen in de EU door middel van innovatieve en duurzame technologieën. Tegen 2030 moet de EU haar huidige datacentrumcapaciteit minimaal verdrievoudigen, waarbij prioriteit wordt gegeven aan energie-efficiënte technologieën in nieuwe installaties. Aangezien de vraag blijft toenemen, moet dit worden beschouwd als een tussentijdse doelstelling, zodat de rekencapaciteit in de EU tegen 2035 aan haar behoeften kan voldoen.

Specifieke doelstelling nr. 2: zorgen voor aantrekkelijke voorwaarden voor de uitrol van duurzame en innovatieve rekencapaciteit. De eerste doelstelling is gericht op de uitrol van capaciteit, terwijl deze is gericht op de voorwaarden voor dergelijke investeringen en uitrolprojecten. Tegen 2030 moet het voor exploitanten in de hele EU mogelijk zijn om alle vergunningen voor de bouw en exploitatie van een datacentrum in minder dan 18 maanden te verkrijgen, inclusief toegang tot land, vergunningen voor toegang tot energie en connectiviteit, wat belangrijke aandachtspunten zijn voor investeerders.

Specifieke doelstelling nr. 3: de algemene afhankelijkheid van niet-Europese cloudcomputingdiensten verminderen. Tegen 2035 moet deze maatregel het marktaandeel van Europese aanbieders van cloudcomputingdiensten op de Europese markt vergroten. Om de strategische autonomie van de Unie te versterken, moet de afhankelijkheid worden verminderd en moet ervoor worden gezorgd dat Europese gebruikers over betrouwbare Europese alternatieven voor niet in Europese gevestigde exploitanten kunnen beschikken. Een sterker Europees aanbod van cloudcomputingdiensten verbetert het vermogen van de Unie om autonoom op te treden en vergroot de veerkracht, het concurrentievermogen en de leveringszekerheid op lange termijn.

Specifieke doelstelling nr. 4: bijdragen tot de bescherming van de openbare orde door het aanbod van cloudcomputingdiensten veerkrachtiger te maken, met name in de overheidssector. Tegen 2035 moet voor het beheer van zeer kritieke gebruiksgevallen in de overheidssector gebruik worden gemaakt van soevereine cloudcomputingdiensten, om de vertrouwelijkheid van gegevens en de operationele autonomie te waarborgen en schade die de openbare orde kan ondermijnen, te voorkomen. Zeer kritieke gebruiksgevallen zijn gevallen van bijzonder systemisch belang die aan essentiële functies ten grondslag liggen of waarbij gevoelige gegevens worden verwerkt. Om strategische autonomie te bereiken, is het cruciaal ervoor te zorgen dat, voor deze gebruiksgevallen, de gegevens worden beschermd en dat de continuïteit van de dienstverlening wordt gewaarborgd. Daarom zijn deze gebruiksgevallen een prioriteit voor de overgang naar diensten waarvan de verlening buiten het bereik van het beleid van derde landen valt dat zou kunnen leiden tot gegevenstoegang of onderbrekingen van de continuïteit van de dienstverlening, d.w.z. soevereine diensten.

1.3.3. *Verwachte resultaten en gevolgen*

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen.

De voorgestelde verordening cloud- en AI-ontwikkeling zal naar verwachting relevante gevolgen hebben voor verschillende begunstigden, waaronder de overheidssector, het Europese cloud- en AI-ecosysteem en burgers. Het initiatief heeft tot doel het cloud- en AI-ecosysteem op het niveau van de Unie te versterken, een voortrekkersrol te spelen op het gebied van energie- en hulpbronnefficiëntie voor datacentra, Europese open cloud- en AI-stacks te ontwikkelen en het gebruik van cloudcomputingdiensten te bevorderen. Dit zal naar verwachting leiden tot de ontwikkeling van geavanceerde AI-technologieën en grensverleggende AI, de versnelling van AI-modellen en -systemen voor industriële doeleinden in strategische sectoren en de ondersteuning van sectoroverschrijdende initiatieven om belangrijke technologische en industriële uitdagingen aan te pakken. Voorts wordt met het voorstel beoogd de uitrol van datacentra in de hele Unie te versnellen, de datacentrumcapaciteit van de EU binnen de komende vijf tot zeven jaar te verdrievoudigen en de uitrol van hulpbronnefficiënte datacentra te waarborgen. De verordening heeft ook tot doel de autonomie te bevorderen, de afhankelijkheid van kritieke technologieën te verminderen en de invoering van cloudcomputingdiensten in de overheidssector te vergroten, zodat kritieke sectoren gebruik kunnen maken van soevereine cloudcomputingdiensten. Daarnaast zal het voorstel leiden tot de oprichting van een Europese cloudfederatie voor de publieke sector, gemeenschappelijke aanbestedingsactiviteiten en de bevordering van opensourceoplossingen. In het algemeen beoogt het voorstel de positie van deze begunstigden te versterken en een concurrerend, innovatief en autonoom Europees

cloud- en AI-ecosysteem te bevorderen dat economische welvaart, sociaal welzijn en strategische autonomie stimuleert. Het voorstel zal naar verwachting positieve effecten hebben op het mondiale concurrentievermogen van de Europese AI- en cloudsector en op de aantrekkelijkheid van de EU voor bedrijven en onderzoekers uit derde landen.

1.3.4. Prestatie-indicatoren

Vermeld de indicatoren voor de monitoring van de voortgang en de beoordeling van de resultaten

Doelstelling 1: meer rekencapaciteit in de EU door middel van innovatieve en duurzame technologieën:

- a) geïnstalleerde rekencapaciteit (MW IT-belasting) per lidstaat;
- b) geaggregeerde rekenkracht voor algemeen gebruik en geoptimaliseerd voor AI, ook gemeten in FLOP's;
- c) aandeel van de EU in de wereldwijd geïnstalleerde rekencapaciteit;
- d) benuttingsgraad van de computercapaciteit van de EU; maatregelen inzake PUE, WUE, locatiegebaseerde emissies en de daarmee samenhangende milieueffecten van datacentra;
- e) uitrol van innovatieve en energie-efficiënte technologieën (lancering van proefprojecten en invoering van nieuwe oplossingen);
- f) aandeel schone energie in datacentra en hergebruik van afvalwarmte;
- g) totale jaarlijkse publieke en particuliere investeringen in in de EU gevestigde datacentra;
- h) aandeel nieuwe datacentrumcapaciteit dat buiten bestaande hubs en in onderbediende regio's wordt uitgerold.

Doelstelling 2: zorgen voor aantrekkelijke voorwaarden voor de uitrol van duurzame en innovatieve rekencapaciteit.

- a) gemiddelde duur vergunningsverlening voor nieuwe datacentrumprojecten;
- b) totale administratieve lasten voor exploitanten;
- c) aandeel projecten dat vertraging oploopt/wordt geannuleerd als gevolg van belemmeringen op het gebied van regelgeving of infrastructuur;
- d) aantal lidstaten met vereenvoudigde vergunningskaders;
- e) index van het kostenconcurrentievermogen.

Doelstelling 3: de afhankelijkheid van niet-Europese cloud- en AI-computingdiensten verminderen:

- a) aandeel Europese aanbieders in de totale inkomsten uit cloudcomputingdiensten in de EU;
- b) aantal overheidsinstanties dat wordt bediend door soevereine aanbieders per lidstaat;
- c) aandeel geïnstalleerde datacentrumcapaciteit in de EU dat eigendom is van Europese aanbieders;
- d) aandeel onbenutte capaciteit in de lidstaten.

Doelstelling 4: bijdragen tot de bescherming van de openbare orde door het aanbod van cloudcomputingdiensten veerkrachtiger te maken, met name in de overheidssector.

- a) aantal gecontroleerde clouddiensten op niveau 2, 3 en 4;
- b) naleving van de soevereiniteitsregeling door aanbestedende diensten (in procenten);

- c) jaarlijkse waarde van de EU-overheidsopdrachten voor soevereine cloudcomputingdiensten;
- d) aantal als open source uit de overheidssector vrijgegeven oplossingen in het register en het aantal downloads ervan door derden.

1.4. Het voorstel/initiatief betreft:

- ☒ een nieuwe actie
- ☐ een nieuwe actie na een proefproject/voorbereidende actie³⁹
- ☐ de verlenging van een bestaande actie
- ☐ de samenvoeging of ombuiging van een of meer acties naar een andere/een nieuwe actie

1.5. Motivering van het voorstel/initiatief

1.5.1. *Behoeften waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief*

De verordening cloud- en AI-ontwikkeling zal naar verwachting binnen 20 dagen na de bekendmaking ervan in het Publicatieblad in werking treden. De inwerkingtreding moet binnen één jaar na publicatie plaatsvinden, met belangrijke uitzonderingen voor voorschriften die een aanvullende overgangperiode vereisen.

1.5.2. *Toegevoegde waarde van de deelname van de EU (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder “toegevoegde waarde van het optreden van de EU” verstaan de waarde die het optreden van de Unie oplevert boven op de waarde die door een optreden van alleen de lidstaten zou zijn gecreëerd.*

De ontwikkeling van de rekencapaciteit in de EU verloopt momenteel langs nationale lijnen. Elke lidstaat werkt binnen een afzonderlijk kader, met verschillende processen en vereisten, voor de uitrol van datacentra, rekening houdend met de lokale omstandigheden en behoeften. Nationaal beleid voor de versnelde uitrol van datacentra dreigt echter te resulteren in verdere versnippering en een “race to the bottom” met betrekking tot duurzaamheid. Bovendien vereist een toenemend aantal toepassingen met een lage latentie een grote rekencapaciteit. Meer in het algemeen wordt de EU geconfronteerd met een tekort aan rekencapaciteit, een probleem dat haar concurrentievermogen negatief dreigt te beïnvloeden en maatregelen op EU-niveau vereist om een regelgevings- en investeringsklimaat in stand te houden dat gemakkelijk te navigeren is voor exploitanten van datacentra en investeerders, ook over de grenzen heen.

Om deze capaciteitskloof te dichten en Europese bedrijven en overheidsdiensten in staat te stellen de rekencapaciteit te benutten en tegelijkertijd de duurzaamheid te waarborgen, zijn maatregelen op EU-niveau nodig. De afhankelijkheid van cloudcomputingdiensten van niet-Europese aanbieders heeft in de hele EU dezelfde onderliggende oorzaken en heeft gevolgen voor bedrijven en overheidsdiensten in alle lidstaten. Europese dienstverleners ondervinden moeilijkheden om in de hele EU op te schalen, bijvoorbeeld als gevolg van de verschillen in nationale betrouwbaarheidsnormen, met name bij overheidsopdrachten. Uiteenlopende

³⁹ In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

ationale aanbestedingspraktijken maken de markt voor Europese aanbieders nog complexer en de onderliggende situatie waarin sprake is van gebrekkige informatievoorziening levert problemen bij de marktwerking op die een respons op EU-niveau vereisen. In de openbare raadpleging werd ook opgeroepen tot EU-maatregelen om deze uitdagingen aan te pakken.

Optreden op EU-niveau heeft naar verwachting een duidelijke meerwaarde om het probleem van de beperkte en geografisch geconcentreerde beschikbaarheid van rekencapaciteit aan te pakken. Door te voorzien in een gemeenschappelijke aanpak voor de uitrol van datacentra, zou op een geografisch evenwichtige manier de coherente planning en uitrol van rekencapaciteit mogelijk moeten worden gemaakt, waarbij een “race to the bottom” wordt vermeden en de complexiteit van de regelgeving voor investeerders en exploitanten van datacentra wordt verminderd. De EU bevindt zich in de unieke positie dat zij ervoor kan zorgen dat het investerings- en versnellingsbeleid een goede weerspiegeling is van de collectieve prioriteiten en versnippering voorkomt. Maatregelen op EU-niveau zouden ervoor zorgen dat alle bedrijven en overheidsinstanties toegang hebben tot voldoende computingcapaciteit om aan hun behoeften te voldoen, en vormen een voorwaarde om van Europa een AI-continent te maken.

Door de afhankelijkheid van cloudcomputingdiensten van niet-Europese aanbieders aan te pakken, is te verwachten dat het optreden op EU-niveau voordelen oplevert die verder reiken dan waar de lidstaten afzonderlijk toe in staat zijn, met name door de problemen bij de marktwerking als gevolg van gebrekkige informatievoorziening aan te pakken. Dit zou de werking van de interne markt verbeteren en aanbieders van cloudcomputingdiensten in staat stellen om tot buiten hun nationale markten te groeien.

1.5.3. *Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan*

Het voorstel is gebaseerd op de praktische ervaring met de uitvoering van bestaande regelgeving op dit gebied. De ervaring heeft geleerd dat juridische waarborgen nodig zijn, maar alleen niet volstaan om de afhankelijkheid van aanbieders van buiten de EU te veranderen. De AVG en de handhaving daarvan door de EDPS hebben overheidsinstanties en aanbieders aangezet tot striktere contractuele bepalingen en strengere regels voor internationale doorgifte. Deze maatregelen hebben echter eerder geleid tot nalevingsoplossingen dan tot concrete veranderingen. Evenzo bleek de noodzaak van gegevenslokalisatie slechts een gedeeltelijke oplossing te bieden voor een aantal van de soevereiniteitsvereisten waarin in specifieke gebruikgevallen moet worden voldaan, met name in de overheidssector. Uit de voorbereidende werkzaamheden voor de Europese cloudcertificeringsregeling (EUCS) is ook gebleken dat er een onderscheid moet worden gemaakt tussen cyberbeveiliging en soevereiniteitsvereisten. De verordening bouwt ook voort op en vormt een aanvulling op de cyberbeveiligingsverordening 2.0 en de bepalingen van de dataverordening, waarbij de nadruk ligt op overstapkosten, interoperabiliteit, overdraagbaarheid en oneerlijke contractvoorwaarden. Tot slot is het voorstel gebaseerd op een uitgebreide strategie voor raadpleging van belanghebbenden.

1.5.4. *Verenigbaarheid met het meerjarig financieel kader en eventuele synergie met andere passende instrumenten*

Het voorstel is verenigbaar met het meerjarig financieel kader, aangezien het in de eerste plaats een nieuw rechtskader zou bieden en tegelijkertijd voor de financiering

gebruikmaakt van bestaande of geplande EU-instrumenten. De belangrijkste financieringssynergieën moeten zijn met tiende kaderprogramma voor onderzoek (KP10) en het Europees Fonds voor concurrentievermogen (EFC), met name in het kader van het beleidsterrein digitaal leiderschap. KP10 moet de onderzoeks- en innovatiedimensie stroomopwaarts in het kader van pijler 1 ondersteunen, terwijl het EFC moet dienen als het belangrijkste uitrolinstrument en zo moet bijdragen tot de omzetting van de onderzoeksresultaten van KP10 in operationele capaciteiten. Andere instrumenten zouden deze inspanningen verder kunnen versterken. Belangrijk projecten van gemeenschappelijk Europees belang (IPCEI's) zouden grootschalige, landsgrensoverschrijdende projecten blijven ondersteunen waarbij cloud-, edge-, chip-, cyberbeveiligings- of AI-infrastructuur de coördinatie tussen lidstaten en particuliere investeringen vereist. Europese consortia voor digitale infrastructuur (EDIC's) kunnen nuttige governance-instrumenten zijn voor groepen lidstaten die gezamenlijk gemeenschappelijke digitale infrastructuur willen exploiteren. Cohesiebeleidsinstrumenten, zoals het Europees Fonds voor regionale ontwikkeling (EFRO) en het Cohesiefonds, dragen bij aan het regionale concurrentievermogen en kunnen dit ondersteunen en pakken territoriale verschillen aan door digitale infrastructuur in minder ontwikkelde regio's mede te financieren. Er worden ook synergieën met InvestEU verwacht door het investeringsklimaat te verbeteren, financierbare projecten te ondersteunen en financieringsinstrumenten aan te vullen om particuliere en publieke investeringen te mobiliseren. In voorkomend geval bouwt het voorstel ook voort op hervormingen en investeringen die zijn uiteengezet in nationale herstel- en veerkrachtplannen, inclusief nationale hervormingsprogramma's en landspecifieke aanbevelingen. Tot slot zouden andere EFC-beleidsvensters sectorspecifieke toepassingen kunnen ondersteunen.

1.5.5. *Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking*

Bij de beoordeling van de beschikbare financieringsopties is rekening gehouden met zowel herschikking binnen de bestaande middelen van de Commissie als de behoefte aan aanvullende financiering. Voor de uitvoering van het initiatief zijn naar schatting in totaal 25 vte's nodig. Daarvan worden 8 vte's van DG DIGIT en 7 vte's van DG CNECT geacht binnen het toepassingsgebied van herschikking te vallen, wat overeenkomt met taken die kunnen worden vervuld door de herprioritering van bestaande activiteiten en het gebruik van bestaande beleidsexpertise. Dit betekent dat 15 van de 25 geraamde vte's door middel van herschikking zouden kunnen worden vervuld. Deze herschikte functies ondersteunen voornamelijk activiteiten die dicht bij bestaande mandaten liggen, zoals beleidscoördinatie, juridische analyse, stakeholderbetrokkenheid, monitoring van de interne markt, programmabeheer, administratieve ondersteuning en samenwerking met de lidstaten. Voor de resterende taken zijn alternatieve financieringsopties onderzocht. Daarbij gaat het onder meer om gerichte versterking van relevante begrotingsonderdelen en het gebruik van bestaande programmabudgetten. Aangezien verschillende taken aanzienlijke operationele kosten met zich mee kunnen brengen, worden echter ook vergoedingen ingevoerd als een belangrijk financieringsmechanisme en om de gevolgen voor de EU-begroting te beperken. Dergelijke vergoedingen waren met name voorzien voor activiteiten in verband met gemeenschappelijke aanbestedingsactiviteiten en het beheer van de Federatie EuroCloud voor het delen van onbenutte capaciteit tussen geïnteresseerde lidstaten.

Voor de resterende 10 vte's zou aanvullende financiering nodig zijn, aangezien deze verband houden met nieuwe of aanzienlijk uitgebreide verantwoordelijkheden die verder reiken dan de huidige veronderstellingen met betrekking tot de werklust.

In het algemeen combineert de voorgestelde aanpak herschikking, financiering op basis van vergoedingen en beperkte aanvullende middelen. Herschikking zou de begrotingsdiscipline en het gebruik van de bestaande deskundigheid van de Commissie waarborgen. Vergoedingen zullen naar verwachting de druk op de EU-begroting verminderen en begrotingsneutraliteit voor de taken die de meeste middelen vergen, ondersteunen. Er worden dus extra kredieten gereserveerd voor nieuwe functies die niet kunnen worden gefinancierd door middel van vergoedingen of interne herschikking.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☐ Beperkte geldigheidsduur

- ☐ Van kracht vanaf [DD/MM/]JJJJ tot en met [DD/MM/]JJJJ;
- ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ voor vastleggingskredieten en vanaf JJJJ tot en met JJJJ voor betalingskredieten;

☒ Onbeperkte geldigheidsduur

- Uitvoering met een opstartperiode vanaf 2028 tot en met 2030,
- gevolgd door een volledige uitvoering.

1.7. Wijzen van uitvoering van de begroting

☒ Direct beheer door de Commissie:

- ☒ door haar diensten, waaronder het personeel in de delegaties van de Unie;
- ☐ door de uitvoerende agentschappen;
 - ☐ Gedeeld beheer met de lidstaten;
 - ☐ Indirect beheer door begrotingsuitvoeringstaken te delegeren aan:
 - ☐ derde landen of de door hen aangewezen organen;
 - ☐ internationale organisaties en hun agentschappen (geef aan welke);
 - ☐ de Europese Investeringsbank en het Europees Investeringsfonds;
 - ☒ de in de artikelen 70 en 71 van het Financieel Reglement bedoelde organen;
 - ☐ overheidsinstanties;
 - ☐ organen met een openbare dienstverleningstaak, voor zover zij zijn voorzien van voldoende financiële garanties;
 - ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;
 - ☐ organen waaraan of personen aan wie de uitvoering van specifieke maatregelen op het gebied van het gemeenschappelijk buitenlands en veiligheidsbeleid in het kader van titel V van het Verdrag betreffende de Europese Unie is toevertrouwd en die worden genoemd in de betrokken basishandeling;
 - ☐ in een lidstaat gevestigde organen die onder het privaatrecht van een lidstaat of onder het Unierecht vallen en die in aanmerking komen om overeenkomstig sectorspecifieke regelgeving te worden belast met de uitvoering van middelen van de Unie of begrotingsgaranties, voor zover dergelijke organen onder zeggenschap staan van overheidsinstanties of privaatrechtelijke organen met een openbare dienstverleningstaak, en beschikken over voldoende financiële garanties in de vorm van hoofdelijke aansprakelijkheid van de controlerende organen of gelijkwaardige financiële garanties, die voor elke actie beperkt kunnen blijven tot het maximumbedrag van de steun van de Unie.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Deze verordening moet binnen vijf jaar na inwerkingtreding worden geëvalueerd en herzien. De Commissie moet aan het Europees Parlement en de Raad verslag uitbrengen over de bevindingen van de evaluatie. Om de consistente uitvoering en monitoring van deze verordening te ondersteunen, moeten de lidstaten er ook voor zorgen dat de relevante informatie over hun activiteiten tijdig beschikbaar is voor de Commissie.

2.2. Beheers- en controlesystemen

2.2.1. *Rechtvaardiging van de voorgestelde wijzen van uitvoering van de begroting, uitvoeringsmechanismen voor financiering, betalingsvoorwaarden en controlestrategie*

De verordening stelt een nieuw beleidskader vast voor geharmoniseerde regels voor de aanbesteding van cloudcomputingdiensten op de interne markt en de uitrol van datacentra in de hele EU, en ondersteunt tegelijkertijd de beleidsdoelstellingen van de Unie op het gebied van consumentenwelzijn, industrieel concurrentievermogen, veiligheid en weerbaarheid, en duurzaamheid. De verordening cloud- en AI-ontwikkeling heeft tot doel de coördinatie van het regelgevingskader voor de ontwikkeling van datacentra en de aankoop van cloudcomputingdiensten te vereenvoudigen en te verbeteren. Deze doelstellingen vereisen een versterkte coördinatie en operationele capaciteit op EU-niveau, die op hun beurt gerichte en evenredige begrotingsmiddelen vereisen. Met het voorstel worden evenredige wijzigingen ingevoerd, waarbij een governancestelsel met nieuwe taken op EU-niveau met een internemarktdimensie wordt ingevoerd en er tegelijkertijd voor wordt gezorgd dat de besluitvorming op het meest efficiënte niveau blijft plaatsvinden. Het gekozen governancemodel heeft tot doel voort te bouwen op bestaande structuren en mandaten, waardoor de behoefte aan nieuwe entiteiten wordt beperkt en de begroting kan worden uitgevoerd door middel van bestaande administratieve en financiële regelingen, wat de kosteneffectiviteit en voorspelbaarheid van de uitgaven waarborgt.

Om deze nieuwe taken uit te voeren, zijn extra personele middelen nodig. Voor de uitvoering en handhaving van de verordening zijn naar schatting 6 extra vte's nodig voor DG CNECT en 4 vte's voor DG DIGIT. De voorgestelde personeelsbezetting is evenredig met de omvang en complexiteit van de nieuwe verantwoordelijkheden en weerspiegelt de meest kostenefficiënte optie, waarbij dubbel werk op nationaal niveau wordt vermeden.

De betalingen volgen de standaardbegrotingsprocedures van de EU, inclusief vastleggingen en betalingen die jaarlijks worden verricht, overeenkomstig het Financieel Reglement en onder de maximumbedragen van het toepasselijke meerjarig financieel kader. Dit wordt ondersteund door de jaarlijkse bijdragen uit de vergoedingen ter dekking van de kosten van aanvullende taken en langetermijncosten. De uitgaven zullen worden onderworpen aan het internecontrolekader van de Commissie, zoals controles vooraf, audits achteraf, prestatie-monitoring en verslaglegging. Dit gebeurt met het oog op een gedegen financieel beheer, de wettigheid en regelmatigheid van de uitgaven en een

doeltreffend gebruik van de middelen van de Unie, terwijl tegelijkertijd een tijdige uitvoering van de verordening wordt gewaarborgd.

2.2.2. *Informatie over de vastgestelde risico's en het systeem of de systemen voor interne controle die zijn opgezet om die risico's te beperken*

Bij de in de handeling voorgestelde activiteiten zijn verschillende entiteiten van de Unie betrokken en sommige uitvoeringsrisico's vereisen inspanningen op het gebied van monitoring, toezicht, coördinatie en begeleiding om deze te beperken. De Commissie zet personeel in voor onder meer het opstellen van richtsnoeren, gedelegeerde handelingen, afhankelijkheidsbeoordelingen, het secretariaat voor het comitologiecomité en het toezicht op de uitvoering van het initiatief, inclusief het monitoren van de voortgang ervan aan de hand van vastgestelde KPI's en mijlpalen. Dit zou het mogelijk maken mogelijke problemen en risico's bij de uitvoering van activiteiten snel in kaart te brengen.

Met name voor de gemeenschappelijke aanbestedingsactiviteiten wordt een stuurgroep opgericht, bestaande uit de Commissie en vertegenwoordigers van de lidstaten, die verantwoordelijk is voor het strategisch toezicht op de aanbestedingsactiviteiten, waaronder de strategische koers van de agenda van aanbestedingsactiviteiten, en de strategische koers van de afzonderlijke aanbestedingsprocedures, waarbij wordt toegezien op de naleving van deze verordening en transparante en niet-discriminerende voorwaarden voor toetreding van aanbestedende diensten. In het geval van de Europese cloudfederatie voor de publieke sector is het belangrijk te zorgen voor een brede deelname van entiteiten van de Unie en tegelijkertijd het hoogste niveau van beveiliging bij de verlening van diensten te waarborgen, in overeenstemming met het recht van de Unie, om de haalbaarheid, doeltreffendheid en continuïteit te waarborgen. Daarom moet de federatie openstaan voor de vrijwillige deelname van instellingen, organen en instanties van de Unie en openbare lichamen uit lidstaten die bereid zijn hun cloudcomputinginfrastructuur met elkaar te verbinden en interoperabele cloudcomputingdiensten in de hele Unie uit te rollen. De Commissie zet een platform op om het delen van datacentra en cloudcomputingcapaciteit die toegankelijk zijn voor haar leden, te vergemakkelijken. Gezien de waarschijnlijke kriticiet en gevoeligheid van de gegevens en toepassingen die in die gedeelde capaciteit worden gehost, moet het platform diensten en mechanismen voor veilige toegang en incidentenbeheer omvatten, zoals gedeeld identiteitsbeheer, instrumenten voor wederzijdse authenticatie en instrumenten voor het melden van incidenten, en ook capaciteiten ter ondersteuning van de werking van de verleende diensten, waaronder monitoring van de dienstverlening, toewijzing van middelen, activering van diensten en prestaties.

2.2.3. *Raming en motivering van de kosteneffectiviteit van de controles (verhouding tussen de controlekosten en de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).*

Er is op het niveau van de Commissie een raming gemaakt van de controlekosten voor dit initiatief. Als bron van deze informatie is het interne beheers- en controlesysteem van de Commissie gebruikt. De kosten zijn geraamd op basis van het personeel en de middelen die worden ingezet voor de in het kader van dit initiatief geplande activiteiten. De verwachte totale kosten voor dergelijke controles kunnen relatief hoog zijn vanwege de complexiteit van de voorgestelde activiteiten en de behoefte aan specifieke middelen om de uitvoeringsrisico's te beperken. De

intensiteit van de controles wordt aangepast aan de aard van de uitgaven, het soort begunstigden of contractanten dat wordt voorzien, het bedrag van de betrokken financiële middelen en het risiconiveau. Voor specifieke activiteiten, zoals gemeenschappelijke aanbestedingen, de Federatie EuroCloud, het financieringsbeheer en het register van soevereine diensten, zijn specifieke middelen en controles nodig, waaronder strategisch toezicht, monitoring en incidentenbeheer. Bij de raming van de kosten van dergelijke controles is ervoor gezorgd dat zij in verhouding blijven tot de waarde van de beheerde middelen, de complexiteit van elke activiteit en de vastgestelde risico's.

Wat het verwachte foutenpercentage betreft, is het de bedoeling dit onder de drempel van 2 % te houden. Dit zal worden bereikt door middel van de bovengenoemde standaardcontroles vooraf en achteraf, zoals verificatie van de subsidiabiliteit en wettigheid van de uitgaven, controles van het aanbestedings- en contractbeheer, monitoring van de te leveren prestaties, risicogebaseerde controles, audits en terugvorderingsprocedures waar nodig. Elke afwijking hiervan zou een gecoördineerde aanpak vereisen en per geval worden besproken.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

De voor deze verordening vereiste aanvullende kredieten zullen onder de bestaande fraudepreventiemaatregelen vallen die van toepassing zijn op de Commissie.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubrieken van het meerjarig financieel kader en betrokken begrotingsonderdelen voor uitgaven

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer	GK/NGK ⁴⁰	van EVA-landen ⁴¹	van kandidaat-lidstaten en potentiële kandidaten ⁴²	van andere derde landen	andere bestemmingsontvangsten
	Rubrieken en begrotingsonderdelen van het MFK nog te bepalen ⁴³	GK/NGK	JA	NEE	NEE	NEE
	Ontvangsten uit vergoedingen (COM int de vergoeding)	GK/NGK	JA	NEE	NEE	JA

- Te creëren nieuwe begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer	GK/NGK	van EVA-landen	van kandidaat-lidstaten en potentiële kandidaten	van andere derde landen	andere bestemmingsontvangsten
	[XX.YY.YY.YY]	GK/NGK	JA/NEE	JA/NEE	JA/NEE	JA/NEE
	[XX.YY.YY.YY]	GK/NGK	JA/NEE	JA/NEE	JA/NEE	JA/NEE
	[XX.YY.YY.YY]	GK/NGK	JA/NEE	JA/NEE	JA/NEE	JA/NEE

⁴⁰ GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

⁴¹ EVA = Europese Vrijhandelsassociatie.

⁴² Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaten van de Westelijke Balkan.

⁴³ De begrotingsonderdelen voor het nieuwe MFK zijn nog niet bekend.

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

- ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig
- ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven

De hieronder vermelde bedragen zijn voorlopig en blijven afhankelijk van het definitieve resultaat van de onderhandelingen over het meerjarig financieel kader (MFK) voor de periode 2028-2034. Dit initiatief zal worden gefinancierd door herschikking binnen de operationele programma's van het volgende MFK, en gedeeltelijk door administratieve uitgaven voor personeel. In dit stadium is het niet mogelijk om de bijdrage van elke MFK-rubriek en elk programma aan te geven, maar verwacht wordt dat een aanzienlijke bijdrage afkomstig zal zijn uit programma's onder rubriek 2 van het MFK 2028-2034 (bv. het Europees Fonds voor concurrentievermogen, met name in het kader van het beleidsterrein “digitaal leiderschap”). Deze ramingen zijn opgesteld op basis van de momenteel beschikbare informatie en zijn bedoeld om nauwkeurige begrotingsramingen te verstrekken.

3.2.1.1. Kredieten uit goedgekeurde begroting

in miljoenen euro's (tot op drie decimalen)

Rubriek van het meerjarig financieel kader			Nummer									
DG CNECT			Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL MFK 2028- 2034	NA 2034	TOTAAL- GENERAAL
			2028	2029	2030	2031	2032	2033	2034			
Beleidskredieten												
Begrotingsonderdeel	Vastleggingen	(1a)	2,386	0,727	2,118	0,427	0,427	0,427	0,427	6,941		6,941
	Betalingen	(2a)	1,193	1,557	1,422	1,272	0,427	0,427	0,427	6,727	0,214	6,941
TOTAAL	Vastleggingen	=1a	2,386	0,727	2,118	0,427	0,427	0,427	0,427	6,941	0,000	6,941

DG CNECT			Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL MFK 2028- 2034	NA 2034	TOTAAL- GENERAAL
			2028	2029	2030	2031	2032	2033	2034			
kredieten voor DG CNECT	Betalingen	=2a	1,193	1,557	1,422	1,272	0,427	0,427	0,427	6,727	0,214	6,941

DG DIGIT			Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL MFK 2028- 2034	NA 2034	TOTAAL- GENERAAL
			2028	2029	2030	2031	2032	2033	2034			
Beleidskredieten												
Begrotingsonderdeel	Vastleggingen	(1a)	2,382							2,382		2,382
	Betalingen	(2a)	1,191	1,191						2,382		2,382
TOTAAL kredieten voor DG DIGIT	Vastleggingen	=1a	2,382	0,000	0,000	0,000	0,000	0,000	0,000	2,382	0,000	2,382
	Betalingen	=2a	1,191	1,191	0,000	0,000	0,000	0,000	0,000	2,382	0,000	2,382

Vanaf 2029 is het VOBV-verzoek het nettobedrag, waarbij de geplande vergoedingen voor de cloudfederatie en gezamenlijke aanbestedingen in mindering zijn gebracht.

Totaal (DIGIT + CNECT)	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL MFK 2028-2034	NA 2034	TOTAAL- GENERAAL
	2028	2029	2030	2031	2032	2033	2034			

TOTAAL beleidskredieten	Vastleggingen	(4)	4,768	0,727	2,118	0,427	0,427	0,427	0,427	9,323	0,000	9,323
	Betalingen	(5)	2,384	2,748	1,422	1,272	0,427	0,427	0,427	9,109	0,214	9,323
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)	0	0	0	0	0	0	0	0	0	0
TOTAAL kredieten onder RUBRIEK 2 van het meerjarig financieel kader	Vastleggingen	=4+6	4,768	0,727	2,118	0,427	0,427	0,427	0,427	9,323	0,000	9,323
	Betalingen	=5+6	2,384	2,748	1,422	1,272	0,427	0,427	0,427	9,109	0,214	9,323

Rubriek van het meerjarig financieel kader	4	“Administratieve uitgaven”
---	---	----------------------------

in miljoenen euro's (tot op drie decimalen)

DG CNECT		Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	TOTAAL MFK 2028-2034
• Personele middelen		1,810	1,810	1,810	1,810	1,810	1,810	1,810	12,670
• Andere administratieve uitgaven		0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
TOTAAL DG CNECT	Kredieten	1,810	1,810	1,810	1,810	1,810	1,810	1,810	12,670

DG: DIGIT		Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	TOTAAL MFK 2028-2034
• Personele middelen		1,794	1,794	1,794	1,794	1,794	1,794	1,794	12,558
• Andere administratieve uitgaven		0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

DG CNECT		Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	TOTAAL MFK 2028-2034
TOTAAL DG DIGIT	Kredieten	1,794	1,794	1,794	1,794	1,794	1,794	1,794	12,558

TOTAAL kredieten onder RUBRIEK 4 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)	3,604	3,604	3,604	3,604	3,604	3,604	3,604	25,228
--	---	-------	-------	-------	-------	-------	-------	-------	--------

in miljoenen euro's (tot op drie decimalen)

		Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	TOTAAL MFK 2028- 2034	NA 2034	TOTAAL GENER AAL
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 4 van het meerjarig financieel kader	Vastleggingen	8,372	4,331	5,722	4,031	4,031	4,031	4,031	34,551	0,000	34,551
	Betalingen	5,988	6,352	5,026	4,876	4,031	4,031	4,031	34,337	0,214	34,551

3.2.1.2. Kredieten gedekt door vergoedingen (EuroCloud en gezamenlijke aanbesteding cloudcomputingdiensten))

in miljoenen euro's (tot op drie decimalen)

Rubriek van het meerjarig financieel kader				Nummer								
DG CNECT			Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL MFK 2028- 2034	NA 2034	TOTAAL- GENERAAL
			2028	2029	2030	2031	2032	2033	2034			
Uit vergoedingen gefinancierde beleidskredieten												
Begrotingsonderdeel	Vastleggingen	(1a)	0,000	2,940	4,410	5,880	2,570	2,570	2,570	20,939		20,939

	Betalingen	(2a)	0,000	2,940	4,410	5,880	2,570	2,570	2,570	20,939		20,939
Uit vergoedingen gefinancierde administratieve kredieten												
Begrotingsonderdeel		(3)										
TOTAAL kredieten	Vastleggingen	=1a+3	0,000	2,940	4,410	5,880	2,570	2,570	2,570	20,939	0,000	20,939
voor DG CNECT	Betalingen	=2a+3	0,000	2,940	4,410	5,880	2,570	2,570	2,570	20,939		20,939

DG DIGIT			Jaar		Jaar		Jaar		Jaar		Jaar		Jaar		TOTAAL MFK 2028-2034	NA 2034	TOTAAL-GENERAAL		
			2028		2029		2030		2031		2032		2033					2034	
Uit vergoedingen gefinancierde beleidskredieten																			
Begrotingsonderdeel	Vastleggingen	(1a)	0,000		3,027		4,317		6,037		6,342		6,663		7,001		33,387		33,387
	Betalingen	(2a)	0,000		3,027		4,317		6,037		6,342		6,663		7,001		33,387		33,387
Uit vergoedingen gefinancierde administratieve kredieten																			
Begrotingsonderdeel		(3)															0		0
TOTAAL kredieten voor DG DIGIT	Vastleggingen	=1a+3	0,000		3,027		4,317		6,037		6,342		6,663		7,001		33,387	0,000	33,387
	Betalingen	=2a+3	0,000		3,027		4,317		6,037		6,342		6,663		7,001		33,387		33,387
			Jaar		Jaar		Jaar		Jaar		Jaar		Jaar		TOTAAL MFK 2028-2034		NA 2034	TOTAAL-GENERAAL	
			2028		2029		2030		2031		2032		2033						2034
TOTAAL beleidskredieten	Vastleggingen	(4)	0,000		5,967		8,727		11,917		8,912		9,233		9,570		54,326	0,000	54,326
	Betalingen	(5)	0,000		5,967		8,727		11,917		8,912		9,233		9,570		54,326		54,326

DG DIGIT			Jaar		Jaar		Jaar		Jaar		Jaar		TOTAAL MFK 2028- 2034	NA 2034	TOTAAL- GENERAAL
			2028		2029		2030		2031		2032				
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)													
TOTAAL kredieten onder RUBRIEK 2 van het meerjarig financieel kader	Vastleggingen	=4+6	0,000	5,967	8,727	11,917	8,912	9,233	9,570	54,326			0,000	54,326	
	Betalingen	=5+6	0,000	5,967	8,727	11,917	8,912	9,233	9,570	54,326			0,000	54,326	

3.2.2. Geraamde output, gefinancierd uit beleidskredieten (niet invullen voor gedecentraliseerde agentschappen)

Vastleggingskredieten, in miljoenen euro's (tot op drie decimalen)

Vermeld doelstellingen en outputs ↓			Jaar 2024		Jaar 2025		Jaar 2026		Jaar 2027		Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						GENERAAL	
	OUTPUTS																	
	Soort 44	Gem. kosten	Aantal	Koste n	Aantal	Koste n	Aantal	Koste n	Aantal	Koste n	Aantal	Koste n	Aantal	Koste n	Aantal	Koste n	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1 ⁴⁵ ...																		
— Output																		
— Output																		
— Output																		

⁴⁴ Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

⁴⁵ Zoals beschreven in punt 1.3.2 “Specifieke doelstellingen”

Subtotaal voor specifieke doelstelling nr. 1																	
SPECIFIEKE DOELSTELLING NR. 2...																	
— Output																	
Subtotaal voor specifieke doelstelling nr. 2																	
TOTAAL																	

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

- ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig
- ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven

3.2.3.1. Kredieten uit goedgekeurde begroting

GOEDGEKEURDE KREDIETEN	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	Jaar	TOTAAL 2028-2034
	2028	2029	2030	2031	2032	2033	2034	
RUBRIEK 4								
Personele middelen	3,604	3,604	3,604	3,604	3,604	3,604	3,604	25.22Ff8
Andere administratieve uitgaven	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Subtotaal RUBRIEK 4	3,604	3,604	3,604	3,604	3,604	3,604	3,604	25,228
Buiten RUBRIEK 4								
Personele middelen	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Andere administratieve uitgaven	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Subtotaal buiten RUBRIEK 4								
GENERAAL	3,604	3,604	3,604	3,604	3,604	3,604	3,604	25,228

De geraamde gevolgen voor de uitgaven en het personeelsbestand voor 2028 en daarna worden louter ter illustratie verstrekt en lopen niet vooruit op het volgende meerjarig financieel kader. De financieringsbron en de omvang van de financiële vastlegging van de Unie voor de periode na 2027 blijven afhankelijk van het resultaat van de interinstitutionele onderhandelingen over het MFK 2028-2034 en zullen daarna worden vastgesteld via de jaarlijkse begrotingsprocedure. Alle kredieten en personeelstoewijzingen vanaf 2028 zijn indicatief.

3.2.3.2. Kredieten uit externe bestemmingsontvangsten

Niet van toepassing.

3.2.3.3. Totaal kredieten

Zie de bovenstaande tabel.

3.2.4. Geraamde personeelsbehoeften

- ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig
- ☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven

3.2.4.1. Gefinancierd uit goedgekeurde begroting

Raming in voltijdequivalenten (vte's)

GOEDGEKEURDE KREDIETEN	Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)							
20 01 02 01 (hoofdkantoor en vertegenwoordigingen van de Commissie)	11	11	11	11	11	11	11
20 01 02 03 (EU-delegaties)	0	0	0	0	0	0	0
01 01 01 01 (onderzoek onder contract)	0	0	0	0	0	0	0

01 01 01 11 (eigen onderzoek)	0	0	0	0	0	0	0
Andere begrotingsonderdelen (te vermelden)	0	0	0	0	0	0	0
• Extern personeel (in vte's)							
20 02 01 (AC, END van de “totale financiële middelen”)	14	14	14	14	14	14	14
20 02 03 (AC, AL, END en JPD in de EU-delegaties)	0	0	0	0	0	0	0
Admin. ondersteuning [XX.01.YY.YY]	— centrale diensten	0	0	0	0	0	0
	— EU-delegaties	0	0	0	0	0	0
01 01 01 02 (AC, END — onderzoek onder contract)	0	0	0	0	0	0	0
01 01 01 12 (AC, END – eigen onderzoek)	0	0	0	0	0	0	0
Andere begrotingsonderdelen (te vermelden) — rubriek 7	0	0	0	0	0	0	0
Andere begrotingsonderdelen (te vermelden) — buiten rubriek 7	0	0	0	0	0	0	0
GENERAAL	25	25	25	25	25	25	25

De geraamde gevolgen voor de uitgaven en het personeelsbestand voor 2028 en daarna worden louter ter illustratie verstrekt en lopen niet vooruit op het volgende meerjarig financieel kader. De financieringsbron en de omvang van de financiële vastlegging van de Unie voor de periode na 2027 blijven afhankelijk van het resultaat van de interinstitutionele onderhandelingen over het MFK 2028-2034 en zullen daarna worden vastgesteld via de jaarlijkse begrotingsprocedure. Alle kredieten en personeelstoewijzingen vanaf 2028 zijn indicatief.

3.2.4.2. Gefinancierd uit externe bestemmingsontvangsten

Niet van toepassing.

3.2.4.3. Totale personeelsbehoeften

Aantal personeelsleden dat nodig is voor de uitvoering van het voorstel (in vte's):

	Uit te voeren door bestaand personeel van de diensten van de Commissie	Uitzonderlijk aanvullend personeel*		
		Te financieren uit rubriek 7 of onderzoek	Te financieren uit BA-onderdeel	Te financieren uit vergoedingen
Personeelsformatieposten	5	6	n.v.t.	
Extern personeel (AC, END, INT)	10	4		

* Het geraamde effect op de uitgaven en het personeel voor 2028 en daarna is indicatief en loopt niet vooruit op het volgende meerjarig financieel kader. De financieringsbron en het toepassingsgebied van de financiële vastleggingen van de Unie in de periode na 2027 blijven afhankelijk van het resultaat van de interinstitutionele onderhandelingen over het meerjarig financieel kader voor de periode 2028-2034 en de jaarlijkse begrotingsprocedure en het coördinatiemechanisme.

In totaal zijn er al 15 vte's aangevraagd voor het initiatief, die als volgt zullen worden herschikt:

- DG CNECT: 2 vte's aan personeelsformatieposten en 5 vte's aan extern personeel;
- DG DIGIT: 3 vte's aan personeelsformatieposten en 5 vte's aan extern personeel;

Naast deze bestaande middelen vereist het initiatief 10 vte's uitzonderlijk extra personeel. Deze vte's bestaan uit 6 ambtenaren en 4 arbeidscontractanten en zijn als volgt verdeeld over DG CNECT en DG DIGIT:

- DG CNECT: 3 vte's aan personeelsformatieposten en 3 vte's aan extern personeel;
- DG DIGIT: 3 vte's aan personeelsformatieposten en 1 vte aan extern personeel.

Die komen boven op de huidige personeelsbezetting om een volledige en doeltreffende uitvoering van het initiatief te waarborgen. De nieuwe taken die met het voorstel worden ingevoerd, kunnen niet worden geabsorbeerd door de bestaande personele middelen van de respectieve DG's. De extra personele middelen die voor dit voorstel nodig zijn, kunnen niet worden vervuld door herschikkingen binnen het DG/de dienst of door herschikkingen uit de beperkte herschikkingspool van de Commissie.

Beschrijving van de nieuwe taken van DG CNECT en DG DIGIT:

Ambtenaren en tijdelijke functionarissen	De ambtenaren en tijdelijke functionarissen hebben de volgende taken: 1. het vaststellen en beheren van de werkprogramma's in het kader van pijler 1 van het initiatief, zoals de ontwikkeling van gedetailleerde projectplannen, begrotingen, toewijzing van middelen, KPI's en monitoringmechanismen; 2. het opstellen van richtsnoeren, gedelegeerde handelingen en afhankelijkheidsbeoordelingen, het oprichten van het secretariaat voor het comitologiecomité en het toezicht houden op de uitvoering van het initiatief, waaronder: a. de ontwikkeling van uitgebreide richtsnoeren, aanbevelingen, modellen en instrumenten om de lidstaten te ondersteunen bij hun uitvoeringsinspanningen met betrekking tot pijler 2 en pijler 3 van het initiatief; b. de ontwikkeling van uitvoeringshandelingen, indien nodig, bijvoorbeeld met betrekking tot de vereisten die van toepassing zijn op de leden van de Federatie EuroCloud en de procedure voor de beoordeling van aanvragen tot toetreding; c. het opstellen van marktmonitoringverslagen om cloudcomputingdiensten te identificeren waarbij de Unie voor dergelijke diensten sterk afhankelijk is van één of een beperkt aantal juridische entiteiten uit derde landen; d. het verzorgen van secretariaatsdiensten, inclusief de ontwikkeling van documenten en verslagen, coördinatie met belanghebbenden; e. de monitoring van de voortgang van het initiatief aan de hand van de vastgestelde KPI's en mijlpalen, de identificatie van mogelijke problemen en risico's en waar nodig het verlenen van technische bijstand en ondersteuning aan de lidstaten; f. het opzetten van een kennisbeheersysteem om beste praktijken, geleerde lessen en deskundigheid in het hele initiatief vast te leggen en uit te wisselen; 3. het opstellen van een bestek voor een externe aanbieder om een register van soevereine diensten op te zetten, te ontwikkelen en bij te houden, en het evalueren en vaststellen van de daaropvolgende governanceprocedures. Na het opzetten moeten regelmatige controles/beoordelingen van een steekproef van gecertificeerde diensten die deel uitmaken van het register, plaatsvinden, inclusief de ontwikkeling van controleprotocollen en beoordelingsmethoden en/of kwaliteitscontroleprocedures om de betrouwbaarheid van de verstrekte informatie te waarborgen; 4. het aanbesteden van het platform voor de Federatie EuroCloud en het ondersteunen van de oprichting van de federatie. De governancemechanismen van
--	--

	de federatie, bv. certificering van vereisten voor lidmaatschap van de federatie, beoordeling van aanvragen van lidstaten en andere openbare lichamen om lid te worden van de federatie, ontwikkeling en handhaving van gemeenschappelijke regels en beleid voor deelname aan de federatie, vallen ook onder hun beheer; 5. het opzetten van systemen die momenteel niet bestaan, als onderdeel van het gezamenlijke aanbestedingskader, waaronder het beheren van de complexiteit van AI-aanbestedingen, betrekkingen met de lidstaten en aanbestedende diensten en het waarborgen dat het kader doeltreffend en efficiënt is. Dit omvat taken zoals het opzetten en beheren van de aanbestedingsprocedures voor cloud-, software- en AI-systemen, het coördineren met deelnemende organisaties en dienstverleners, het beheren van de contracten en overeenkomsten met dienstverleners en het waarborgen van de naleving van de regelgeving en het beleid van de EU; 6. het ontwikkelen en onderhouden van betrekkingen met belanghebbenden, waaronder de lidstaten, vertegenwoordigers van de betrokken sectoren en andere relevante partijen, om ervoor te zorgen dat het initiatief goed gecoördineerd en doeltreffend is en inspeelt op de behoeften van de belanghebbenden, zoals het organiseren van regelmatige bijeenkomsten, workshops en conferenties om de communicatie en samenwerking te vergemakkelijken. Dit omvat ook nauwe samenwerking met de bevoegde autoriteiten op het gebied van onderzoeks- en handavingsmaatregelen om de naleving van titel IV van de handeling te waarborgen.
Extern personeel	Extern personeel zal worden belast met: 1. het regelmatig beheren van de in het kader van de werkprogramma's van pijler 1 toegekende projecten, zoals de monitoring van de voortgang ervan, coördinatie met begunstigen en verificatie van de projectresultaten en mijlpalen, om ervoor te zorgen dat deze tijdig, binnen de begroting en met de vereiste kwaliteitsnormen worden geleverd. Het initiatief wordt in het volgende MFK uitgevoerd en bouwt voort op de resultaten van bestaande projecten die reeds zijn goedgekeurd in het kader van Horizon Europa en het programma Digitaal Europa, zoals Simpl en de Gemeenschappelijke Onderneming "Slimme netwerken en diensten", onder meer in coördinatie met andere eenheden; 2. het opzetten en toepassen van ondersteuningsmechanismen om de lidstaten richtsnoeren te verstrekken voor de uitrol van zones voor de versnelde uitrol van datacentra, met name tijdens de eerste twee jaar van het initiatief. Dit omvat de verlening van ad-hocsteun aan de lidstaten bij de ontwikkeling en uitvoering van hun nationale strategieën en plannen. Na de eerste periode zal dit een meer ad hoc coördinerende rol worden, waarbij de nadruk ligt op het verlenen van gerichte steun aan de lidstaten waar nodig, en ervoor wordt gezorgd dat het initiatief blijft afgestemd op de behoeften en prioriteiten van de belanghebbenden; 3. het jaarlijks opzetten en beheren van een studie om de rekencapaciteit in heel Europa te monitoren, waaronder het vaststellen van het toepassingsgebied en de methode van de studie, het verifiëren van de verzamelde gegevens en het evalueren van de te leveren prestaties; 4. het beheren van de gezamenlijke aanbestedingsactiviteiten, met name met betrekking tot strategische inkoop en marktforming, d.w.z. het kantoor voor leveranciersbeheer en het opstellen van specificaties en technische vereisten voor cloud-, AI- en softwarediensten; 5. het jaarlijks beheren van het register van soevereine diensten, onder meer door toezicht te houden op de activiteiten van de contractant die verband houden met de activiteiten van het register, waaronder technisch projectbeheer, d.w.z. ervoor zorgen dat de contractant het register levert overeenkomstig de overeengekomen technische specificaties, tijdschema's en begroting, en tegelijkertijd toezicht houden op de processen van de contractant om ervoor te zorgen dat het register aan de vereiste normen voldoet; 6. het beheren van de externe contractant die elk jaar de administratieve, technische en operationele activiteiten van het platform voor de Federatie EuroCloud uitvoert, alsook de technische aspecten van het platform voor de Federatie EuroCloud, zoals het toezicht op de technische architectuur en infrastructuur.

3.2.5. Overzicht van het geschatte effect op met digitale technologie samenhangende investeringen

Verplicht: in onderstaande tabel moet de beste schatting worden gegeven van de met digitale technologie samenhangende investeringen die uit het voorstel/initiatief voortvloeien.

De kredieten onder rubriek 7 moeten in uitzonderlijke gevallen in het desbetreffende onderdeel worden opgenomen, indien vereist voor de uitvoering van het voorstel/initiatief.

De kredieten onder de rubrieken 1 t/m 6 moeten worden weergegeven als “IT-beleidsuitgaven inzake operationele programma’s”. Deze uitgaven betreffen het operationele budget dat gebruikt moet worden voor hergebruik, koop of ontwikkeling van IT-platforms of tools die rechtstreeks verband houden met de uitvoering van het initiatief, alsook daarmee verband houdende investeringen (bv. licenties, studies, gegevensopslag enz.). De in deze tabel vermelde informatie moet in overeenstemming zijn met de gegevens in deel 4, “Digitale dimensies”.

TOTAAL Digitale en IT- kredieten	Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	TOTAAL MFK 2028-2034
RUBRIEK 4								
IT-uitgaven (algemeen)	0	0	0	0	0	0	0	0
Subtotaal RUBRIEK 4	0	0	0	0	0	0	0	0
Buiten RUBRIEK 4								
IT- beleidsuitgaven inzake operationele programma's	0	0	0	0	0	0	0	0
Subtotaal buiten RUBRIEK 4	0	0	0	0	0	0	0	0
GENERAAL	0	0	0	0	0	0	0	0

3.2.6. Verenigbaarheid met het huidige meerjarig financieel kader

Het voorstel/initiatief:

- ☒ kan volledig worden gefinancierd door middel vanerschikking binnen de relevante rubriek van het meerjarig financieel kader (MFK)

Onverminderd de onderhandelingen over het volgende MFK zullen vanaf 2028 aan de aan de verordening cloud- en AI-ontwikkeling gerelateerde activiteiten toegewezen kredieten worden gedekt viaerschikkingen uit de uitgebreide kredietfaciliteit in het kader van het MFK 2028-2034 en gedeeltelijk via vergoedingen.

- ☐ vereist een beroep op de niet-toegewezen marge in de desbetreffende rubriek van het MFK en/of op de speciale instrumenten zoals gedefinieerd in de MFK-verordening
- ☐ vereist een herziening van het MFK

3.2.7. Bijdragen van derden

Het voorstel/initiatief:

- ☒ voorziet niet in medefinanciering door derden
- ☐ voorziet in medefinanciering door derden, zoals hieronder wordt geraamd:

Kredieten in miljoenen euro's (tot op drie decimalen)

	Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034	Totaal
Vermeld medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

3.3. Geraamde gevolgen voor de ontvangsten

- ☐ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.
- ☒ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:
 - ☐ voor de eigen middelen
 - ☐ voor overige ontvangsten
 - ☒ geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven

in miljoenen euro's (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief ⁴⁶						
		Jaar 2028	Jaar 2029	Jaar 2030	Jaar 2031	Jaar 2032	Jaar 2033	Jaar 2034
Vergoeding voor gezamenlijke aanbesteding cloudcomputingdiensten (DG DIGIT)		0,000	3,027	4,317	6,037	6,342	6,663	7,001
Vergoeding cloudfederatie (DG CNECT)		0,000	2,940	4,410	5,880	2,570	2,570	2,570

⁴⁶ Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.

Vermeld voor de toegewezen ontvangsten de betrokken begrotingsonderdelen voor uitgaven.

Vergoeding voor gezamenlijke aanbesteding cloudcomputingdiensten:

De bestemmingsontvangsten zullen worden gebruikt ter dekking van de begrotingsuitgaven in verband met het bemiddelingssysteem dat is opgezet voor de gezamenlijke aanbestedingsregeling. De ontvangsten zullen worden toegewezen ter ondersteuning van de operationele kosten van het systeem, inclusief de kosten van extern personeel, instrumenten en systemen.

De verdeling van de bestemmingsontvangsten is gemiddeld als volgt: ongeveer 50 % wordt toegewezen ter dekking van operationele en administratieve kosten, bv. studies en onderzoek ter onderbouwing van aanbestedingsbesluiten, instrumenten en systemen voor gemeenschapsbeheer ter ondersteuning van communicatie en samenwerking tussen deelnemende organisaties, technische hulpmiddelen en platformintegratie; ongeveer 30 % wordt toegewezen ter dekking van de kosten van de ontwikkeling en het onderhoud van de nodige instrumenten en systemen, zoals aanbestedingsplatforms en marktplaatsen, systemen voor het levenscyclusbeheer van opdrachten, instrumenten voor portefeuille- en vraagbeheer; ongeveer 20 % wordt toegewezen ter dekking van de kosten van extra gespecialiseerd extern personeel, bv. voor de aankoop van software, gegevensbeschermingsactiviteiten, backoffice, FinOps en ContractOps voor het beheer van contractuele aspecten, portefeuille- en vraagbeheer.

Deze toewijzing moet ervoor zorgen dat de bestemmingsontvangsten alleen worden gebruikt om de operationele kosten van het systeem en de begrotingsuitgaven in verband met het bemiddelingssysteem te dekken. Deze kosten worden toegewezen op basis van de daadwerkelijke vraag, waarbij ervoor wordt gezorgd dat de middelen efficiënt worden gebruikt om de regeling voor gezamenlijke aanbestedingen te ondersteunen.

Vergoeding cloudfederatie:

De bestemmingsontvangsten worden gebruikt ter dekking van de begrotingsuitgaven in verband met de diensten en het platform die voor de Federatie EuroCloud zijn opgezet. De ontvangsten zullen worden toegewezen ter ondersteuning van de operationele kosten van het systeem, inclusief de kosten van extern personeel, instrumenten en systemen.

De uitgaven die nodig zijn om de federatie te financieren, bestaan uit operationele en ontwikkelingsgerelateerde kosten. Een aanzienlijk deel heeft betrekking op de ontwikkeling en het onderhoud van het platform. De ontwikkelingskosten zullen naar verwachting het hoogst zijn in de eerste jaren, als gevolg van de initiële uitrolfase. Vanaf jaar 4 dekken de kosten de lopende activiteiten, technische ondersteuning en periodieke upgrades. Het onderhoudscontract omvat kwaliteitsborging en prestatiebeoordeling door een externe contractant, waarvan de kosten worden geraamd op ongeveer 10 % van de totale aanbestedingswaarde, op basis van soortgelijke aanbestedingscontracten. De operationele kosten omvatten de kosten van externe technische deskundigen (10 profielen) boven op de interne vte's die verantwoordelijk zouden zijn voor de coördinatie en het projectbeheer (zie hierboven onder de beschrijving van nieuwe taken die door DG CNECT moeten worden uitgevoerd). Hun rol wordt geleidelijk groter, met ongeveer 40 % van de capaciteit in jaar 1, 80 % in jaar 2, om vanaf jaar 3 volledige capaciteit te bereiken, in

overeenstemming met de toenemende operationele behoeften van de federatie. Verdere uitgaven omvatten kosten voor de IT-infrastructuur, zoals hostingdiensten en beveiligingsgerelateerde instrumenten, die nodig zijn om de betrouwbaarheid, schaalbaarheid en bescherming van het platform te waarborgen.

Deze toewijzing moet ervoor zorgen dat de bestemmingsontvangsten worden gebruikt om de operationele kosten van het systeem en de begrotingsuitgaven in verband met de geleverde diensten te dekken. Deze kosten worden toegewezen op basis van de daadwerkelijke vraag, waarbij ervoor wordt gezorgd dat de middelen efficiënt worden gebruikt om de Federatie EuroCloud te ondersteunen. De initiële opstartkosten kunnen ten laste komen van de algemene begroting van de Unie en gedurende een bepaalde periode door de deelnemende autoriteiten worden terugbetaald via de vergoedingen.

Andere opmerkingen (bv. over de methode/formule voor de berekening van de gevolgen voor de ontvangsten of andere informatie).

Vergoeding voor gezamenlijke aanbesteding cloudcomputingdiensten:

De vergoeding is bedoeld om de operationele kosten voor de aanbestedingsactiviteiten (interinstitutionele aanbesteding, gezamenlijke aanbesteding en aankoopcentrales) en de mogelijke aanvullende aanbestedingsactiviteiten te dekken.

De vergoeding wordt betaald door de deelnemende aanbestedende diensten. De vergoeding zou de prijs voor de aanbestedende diensten verhogen. De prijs wordt echter zodanig vastgesteld dat alleen de noodzakelijke kosten voor het beheer van de aanbestedingsactiviteiten worden gedekt, aangezien deze gemeenschappelijke aanbesteding tot doel heeft te kunnen onderhandelen over betere voorwaarden, lagere prijzen voor alle aanbestedende diensten te bedingen en de invoering op grote schaal van voortdurend evoluerende technologieën te vergemakkelijken.

De vergoedingen worden pro rata berekend per transactie of via een vaste vergoeding per volgende gegunde opdracht, zoals gespecificeerd in het aanbestedingsdocument. De vergoedingen worden berekend op basis van een jaarlijkse prognose van het verbruik van de begunstigden en worden jaarlijks vóór de uitvoering van de opdrachten geïnd. De aan de deelnemende aanbestedende diensten aangerekende vergoedingen mogen de door de Commissie gemaakte, verifieerbare kosten niet overschrijden. De vergoeding wordt jaarlijks herberekend in verhouding tot de omvang van de geplande werkzaamheden en de gemaakte kosten. De inning van de vergoeding begint vanaf 2029, zodat een initieel opzetproces mogelijk is. De vergoeding wordt geïnd via bestaande onlinediensten voor het factureren en innen van betalingen van deelnemende aanbestedende diensten.

De geraamde jaarlijkse ontvangsten zijn afhankelijk van zowel het aantal deelnemende autoriteiten (begunstigden) als hun gemiddelde verwachte aankopen. De ontvangsten uit vergoedingen zullen ongeveer 6 miljoen EUR per jaar moeten bedragen om de geraamde gemiddelde jaarlijkse kosten te dekken. Op basis van ramingen van de deelname moet dit haalbaar zijn met een gemiddeld jaarlijks vergoedingspercentage van 2 % dat wordt toegepast op de uitgaven per autoriteit. Als de totale uitgaven dit niveau overschrijden, bijvoorbeeld omdat meer autoriteiten deelnemen, de gemiddelde uitgaven per autoriteit hoger zijn, of beide, wordt het vergoedingstarief evenredig verlaagd. De ontvangsten uit de vergoeding worden

gebruikt voor de financiering van alle operationele kosten van het aanbestedingsmechanisme, zoals hierboven uiteengezet.

De Commissie brengt aan het Europees Parlement en de Raad verslag uit over het totaalbedrag van de voor de aanbestedingsactiviteiten gemaakte kosten en het totaalbedrag van de aangerekende vergoedingen.

Vergoeding cloudfederatie:

De vergoeding is bedoeld om de operationele kosten te dekken voor de oprichting en het beheer van de Federatie EuroCloud, inclusief de beoordeling van lidmaatschapsaanvragen en het vergemakkelijken van het delen van datacentrum- en cloudcomputingdiensten door de ontwikkeling van het platform voor de Federatie EuroCloud.

De vergoeding wordt betaald door de leden van de federatie. De vergoeding zou de totale kosten voor de deelnemers licht verhogen. Ze moet echter strikt worden bepaald om de noodzakelijke administratieve en operationele kosten van de werking van de federatie te dekken. Dit leidt naar verwachting tot efficiëntieverbeteringen en kostenbesparingen. Door leden in staat te stellen capaciteit uit te wisselen en gebruik te maken van middelen die anders onbenut zouden blijven, kunnen deelnemers toegang krijgen tot diensten tegen gunstigere tarieven dan die welke op de open markt beschikbaar zijn. Dit uitwisselingsmodel kan de behoefte aan externe aanbestedingen verminderen en de totale benuttingsgraad van middelen verbeteren, met name op korte tot middellange termijn. Hoewel de vergoeding marginale kosten met zich meebrengt, wordt zij gecompenseerd door de economische voordelen die voortvloeien uit samenwerking, een hogere benuttingsgraad en meer concurrerende prijzen binnen de federatie.

De Commissie stelt uitvoeringshandelingen vast met gedetailleerde regels voor het bepalen van de door Commissie aan te rekenen vergoedingen, waarin de geraamde kosten worden gespecificeerd die zijn toe te schrijven aan de activiteiten waarvoor vergoedingen worden aangerekend, en de individuele aan te rekenen vergoedingsbedragen, alsook de manieren waarop en de voorwaarden waaronder de vergoedingen moeten worden betaald.

De lidmaatschapsbijdrage wordt gestructureerd als een kostendekkingsmechanisme dat in verhouding staat tot het aantal deelnemende entiteiten in de federatie. Het doel is de kosten te dekken en tegelijkertijd de financiële lasten voor elk lid geleidelijk te verminderen naarmate de deelname toeneemt.

Aangenomen wordt dat het gebruik mettertijd zal toenemen, waarbij ongeveer 20 % van de mogelijke entiteiten zich in het eerste jaar zal aansluiten, 40 % in het tweede jaar, 60 % in het derde jaar en ongeveer 80 % in het vierde jaar, alvorens in het vijfde jaar volledige deelname te bereiken. Het eerste jaar is gewijd aan de oprichting van de federatie, zodat er geen volledige lidmaatschapsbijdrage van toepassing is. Op basis van de schattingen kan de lidmaatschapsbijdrage vanaf het tweede jaar worden vastgesteld op ongeveer 75 000 EUR per lid, wat het relatief lage aantal deelnemers weerspiegelt. Naarmate meer entiteiten toetreden en de kostenbasis over een grotere groep wordt verdeeld, kan de vergoeding geleidelijk dalen tot ongeveer 30 000 EUR per lid zodra de volledige capaciteit is bereikt. Verwacht wordt dat de regeling rond het vierde jaar een evenwichtspoint bereikt. In dat stadium stabiliseert de vergoedingsstructuur zich op een niveau dat toereikend is om de activiteiten in stand

te houden zonder een aanzienlijk overschot te genereren, in overeenstemming met het beginsel van kostendekking.

De inning van de vergoeding begint vanaf 2029, zodat een initieel opzetproces mogelijk is. De vergoeding wordt geïnd via onlinediensten voor het factureren en innen van betalingen van deelnemende diensten.

De geraamde jaarlijkse ontvangsten hangen af van het aantal deelnemende leden en de toepasselijke lidmaatschapsbijdrage. Op basis van een gemiddelde lidmaatschapsbijdrage van ongeveer 75 000 EUR per lid komen de jaarlijkse inkomsten op ongeveer 4,4 miljoen EUR per jaar, om de geraamde gemiddelde jaarlijkse exploitatiekosten van de federatie, inclusief de initiële vaste kosten, te dekken. Naarmate de deelname toeneemt, worden de beheerskosten van de federatie over een groter aantal leden verdeeld. Bijgevolg daalt dan de vergoeding per lid evenredig, waarbij de jaarlijkse ontvangsten zich op een lager niveau stabiliseren, bv. op ongeveer 2,6 miljoen EUR per jaar.

De Commissie brengt aan het Europees Parlement en de Raad verslag uit over het totaalbedrag van de voor de activiteiten van de federatie gemaakte kosten en het totaalbedrag van de aangerekende vergoedingen. De verslagleggingsperiode moet nog worden vastgesteld.

Het gebruik van bestemmingsontvangsten voor de gezamenlijke aanbesteding en de Federatie EuroCloud biedt op het gebied van het begrotingsbeleid kansen om te zorgen voor een specifieke en stabiele financieringsstroom voor deze initiatieven. Door de ontvangsten uit de vergoeding voor specifieke doeleinden te bestemmen, kan de Commissie garanderen dat de middelen efficiënt en doeltreffend worden gebruikt om de ontwikkeling van een Europees cloud-ecosysteem te ondersteunen. Deze aanpak wordt gerechtvaardigd door de noodzaak om te voorzien in een duidelijk en voorspelbaar financieel kader voor beide initiatieven in het kader van de wetgevingshandeling inzake cloud- en AI-ontwikkeling, waardoor deze op strategische wijze en voor de lange termijn kunnen worden gepland en uitgevoerd.

Wat de naleving van de begrotingsbeginselen van universaliteit en eenheid betreft, wordt het gebruik van bestemmingsontvangsten gerechtvaardigd door het feit dat deze initiatieven zijn ontworpen ter ondersteuning van specifieke en duidelijk omschreven beleidsdoelstellingen, d.w.z. de ontwikkeling van een Europees cloud-ecosysteem voor het delen van onbenutte capaciteit tussen de lidstaten en de gezamenlijke aankoop van clouddiensten om efficiëntie en schaalvoordelen te bereiken. De ontvangsten uit de vergoedingen worden gebruikt voor de financiering van specifieke uitgaven die rechtstreeks verband houden met de verwezenlijking van deze doelstellingen, zoals hierboven gespecificeerd in de respectieve afdelingen die betrekking hebben op beide activiteiten. Door gebruik te maken van bestemmingsontvangsten kan de Commissie ervoor zorgen dat de middelen doelgericht en efficiënt worden gebruikt, zonder negatieve gevolgen voor het algemene evenwicht van de begroting van de Unie. Voorts is het gebruik van bestemmingsontvangsten in overeenstemming met het eenheidsbeginsel, aangezien het de Commissie in staat stelt deze initiatieven op coherente en gecoördineerde wijze uit te voeren, waarbij dubbel werk wordt vermeden en ervoor wordt gezorgd dat de middelen worden gebruikt ter ondersteuning van een gemeenschappelijke Europese doelstelling. De Commissie zorgt er ook voor dat het gebruik van bestemmingsontvangsten transparant en controleerbaar is, met regelmatige verslaglegging over en evaluatie van de voortgang en het effect van het initiatief.

Daarnaast houdt de Commissie rekening met de noodzaak om mogelijke verstoringen of ongelijkheden in de behandeling van verschillende aanbieders van clouddiensten te voorkomen, en zorgt zij ervoor dat het gebruik van bestemmingsontvangsten eerlijk, evenredig en niet-discriminerend is. De Commissie pleegt ook overleg met relevante belanghebbenden om ervoor te zorgen dat het initiatief zodanig wordt ontworpen en uitgevoerd dat het inspeelt op hun behoeften en punten van zorg.

Het is belangrijk op te merken dat alleen de operationele kosten van de twee initiatieven, zoals hierboven beschreven, worden gedekt door de bestemmingsontvangsten die door de vergoedingen worden gegenereerd. De administratieve kosten worden daarentegen niet gedekt door de bestemmingsontvangsten.

Voor het geval dat de veronderstelde bedragen van de vergoedingen niet of niet op het veronderstelde tijdstip worden ontvangen, volgt de Commissie een voorzichtige aanpak om de risico's te beperken. In het geval van gezamenlijke aanbestedingen betekent het dat, als de vergoedingen niet worden betaald, er geen systeem wordt opgezet en dat het initiatief geen aanzienlijke kosten met zich meebrengt. Anderzijds bouwt de Federatie EuroCloud voort op reeds bestaande studies en bewijs van de belangstelling van de lidstaten voor dit initiatief. Bovendien worden de grote kosten in verband met het initiatief reeds gedekt door het huidige meerjarig financieel kader in het kader van de begroting die reeds aan de Commissie is toegewezen, waardoor dit financiële risico in zijn geheel wordt beperkt. In het algemeen stelt deze aanpak de Commissie in staat haar plannen aan te passen zonder aanzienlijke financiële risico's te lopen, en flexibeler te zijn om de toewijzing van middelen waar nodig aan te passen, teneinde het succes van deze initiatieven te waarborgen.

4. DIGITALE DIMENSIES

4.1. Voorschriften met digitale relevantie

Korte beschrijving van de voorschriften met digitale relevantie en de categorieën ervan (data, procesdigitalisering en -automatisering, digitale oplossingen en/of digitale overheidsdiensten).

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
TITEL II ONDERZOEKS-, ONTWIKKELINGS- EN UITROLACTIVITEITEN VOOR HET CLOUD- EN AI- ECOSYSTEEM <i>Artikel 7 Nationale cloud- en AI- strategieën</i>	De lidstaten doen aan de Commissie kennisgeving van hun nationale strategieën	Europese Commissie Nationale bevoegde autoriteiten	Kennisgeving	Gegevens
TITEL III DATACENTRUMCAPACITEIT <i>Artikel 14 Aanwijzing van strategische datacentrumprojecten</i>	Aanvragen voor de aanwijzing van een strategisch datacentrumproject bevatten alle nodige en relevante informatie om aan te tonen dat het project aan de relevante criteria voldoet.	Uitvoerders project Europese Commissie	Monitoring van inzichten in de aanvragen	Gegevens
TITEL III DATACENTRUMCAPACITEIT <i>Artikel 15 Monitoring van de capaciteitskloof</i>	De Commissie monitort de in de Unie beschikbare rekencapaciteit, inclusief de edgecomputingcapaciteit; het volume van de vraag naar datacentrumcapaciteit; de omvang van het capaciteitstekort.	Europese Commissie Nationale bevoegde autoriteiten	Gegevensverzameling	Gegevens
TITEL IV	Een aanbieder van cloudcomputingdiensten die wil worden	Aanbieders van	Toezihtsmechanisme	Gegevens

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	erkend als aanbieder van een Uniebetrouwbaarheidsniveau, dient een erkenningsaanvraag in bij de nationale bevoegde autoriteit van vestiging.	cloudcomputingdiensten Nationale bevoegde autoriteiten		
TITEL IV AUTONOMIE <i>Artikel 19 Conformiteitszelfbeoordeling</i>	De aanbieder van cloudcomputingdiensten kan een conformiteitszelfbeoordeling afgeven om de naleving van Uniebetrouwbaarheidsniveau 1 aan te tonen. Deze moeten openbaar worden gemaakt.	Aanbieders van cloudcomputingdiensten Nationale bevoegde autoriteiten Europese Commissie	Toezihtsmechanisme	Gegevens
TITEL IV AUTONOMIE <i>Artikel 20 Onafhankelijke controle</i>	Voorziet in de mogelijkheid van onafhankelijke controles voor de Uniebetrouwbaarheidsniveaus 2, 3 en 4. Bepalingen met betrekking tot gegevensaspecten in het kader van dergelijke controles.	Aanbieders van cloudcomputingdiensten Controleorganisaties Europese Commissie	Toezihtsmechanisme	Gegevens
TITEL IV AUTONOMIE <i>Artikel 21 Inhoud en kwaliteit van controlebewijs</i>	De controles moeten zijn gebaseerd op de bijlagen II (Criteria voor Uniebetrouwbaarheidsniveaus) en III (Controlebewijs voor de controleprocedure) Moeten voldoende volledig en betrouwbaar zijn.	Aanbieders van cloudcomputingdiensten Controleorganisaties Europese Commissie	Gegevenskwaliteit	Gegevens
TITEL IV AUTONOMIE <i>Artikel 22 Centraal register van</i>	De Commissie zorgt voor het opzetten en bijhouden van een specifiek register van cloudcomputingdiensten die zijn erkend op basis van een	Europese Commissie Nationale bevoegde autoriteiten	Databank	Digitale oplossing Gegevens

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
<i>cloudcomputingdiensten</i>	Uniebetrouwbaarheidsniveau. De controlerende nationale bevoegde autoriteit van vestiging registreert de gecontroleerde diensten in het centrale register. Elke intrekking van een erkenning wordt in het centrale register bekendgemaakt en blijft gedurende 5 jaar openbaar. Het centrale register wordt openbaar gemaakt door de Commissie en regelmatig bijgewerkt door de Commissie en de nationale bevoegde autoriteiten van vestiging op een speciale en gemakkelijk toegankelijke website.			Digitale overheidsdienst

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
TITEL IV AUTONOMIE <i>Artikel 23</i> <i>Transparantieverplichtingen</i>	Zodra de aanbieder van de dienst kennis krijgt van informatie of materiële wijzigingen in de omstandigheden met betrekking tot de cloudcomputingdiensten die van invloed kunnen zijn op het controlerapport/-advies, stelt hij de controleorganisatie en de nationale bevoegde autoriteit van vestiging daarvan onverwijld in kennis. Indien de resultaten van het controlerapport en -advies moeten worden gewijzigd of ingetrokken, stelt de controleorganisatie de nationale bevoegde autoriteit en de Commissie daarvan onverwijld in kennis. Indien de resultaten van de erkenning moeten worden gewijzigd of ingetrokken, stelt de nationale bevoegde autoriteit van vestiging de nationale bevoegde autoriteiten van de andere lidstaten en de Commissie daarvan onverwijld in kennis.	Aanbieders van cloudcomputingdiensten Controleorganisaties Nationale bevoegde autoriteiten Europese Commissie	Kennisgeving	Gegevens
TITEL IV AUTONOMIE <i>Artikel 24</i>	De lidstaten stellen de Commissie zo spoedig mogelijk in kennis van de regels inzake sancties en schadevergoeding en van alle latere wijzigingen daarvan.	Nationale bevoegde autoriteiten Europese Commissie	Kennisgeving	Gegevens

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
<i>Sancties en schadevergoeding</i>				
TITEL IV AUTONOMIE <i>Artikel 25 Nationale bevoegde autoriteiten</i>	Elke lidstaat wijst een of meer nationale bevoegde autoriteiten aan. De lidstaten geven de lijst van autoriteiten door aan de Commissie. De Commissie houdt een openbaar register van deze autoriteiten bij.	Europese Commissie Nationale bevoegde autoriteiten	Aanwijzing van bevoegde autoriteiten	Gegevens
TITEL IV AUTONOMIE <i>Artikel 27 Wederzijdse bijstand</i>	Gegevens worden gebruikt in het kader van de samenwerking tussen nationale bevoegde autoriteiten .	Nationale bevoegde autoriteiten Europese Commissie	Gegevensuitwisseling	Gegevens
TITEL IV AUTONOMIE <i>Artikel 89 Landsgrensoverschrijdende samenwerking</i>	Er worden gegevens uitgewisseld in het kader van landsgrensoverschrijdende samenwerking .	Nationale bevoegde autoriteiten Europese Commissie	Gegevensuitwisseling	Gegevens
TITEL IV AUTONOMIE <i>Artikel 29 Risicobeoordelingen</i>	De lidstaten moeten een of meer risicobeoordelingen uitvoeren , waarbij zoveel mogelijk rekening wordt gehouden met de richtsnoeren van de Commissie. De lidstaten geven de resultaten van de risicobeoordelingen door aan de Commissie .	Lidstaten Europese Commissie Aanbieders van clouddiensten	Risicobeoordeling	Gegevens

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
	Voor de toepassing van de richtsnoeren heeft de Commissie het recht om informatie op te vragen bij aanbieders van clouddiensten.			
TITEL IV AUTONOMIE <i>Artikel 33 Monitoring van aanbesteding voor innovatie op het gebied van cloud en AI</i>	De lidstaten delen de Commissie jaarlijks bepaalde informatie mee met betrekking tot de monitoring van aanbestedingen voor innovatieve cloudcomputingdiensten en AI-systemen.	Lidstaten Europese Commissie	Verslaglegging	Gegevens
TITEL IV AUTONOMIE <i>Artikel 34 Oprichting van de Europese cloudfederatie voor de publieke sector</i>	De Commissie richt een platform op voor de Federatie EuroCloud.	Europese Commissie Entiteiten van de Unie Openbare lichamen	Vereisten voor een digitale oplossing	Digitale overheidsdienst Digitale oplossing
TITEL IV AUTONOMIE <i>Artikel 37 Aanbestedingsactiviteiten van de Commissie</i>	De Commissie kan een gemeenschappelijk aanbestedingsplatform oprichten en beheren, waaronder diensten die kunnen worden gebruikt om de uitvoering van de aanbestedingsactiviteiten uit hoofde van dit hoofdstuk te vergemakkelijken.	Europese Commissie	Vereisten voor een digitale oplossing	Digitale oplossing
TITEL IV AUTONOMIE <i>Artikel 42 Delen en hergebruiken</i>	Wanneer een entiteit van de Unie of een openbaar lichaam in het kader van een opensourcelicentie software waarop zij	Entiteiten van de Unie Openbare lichamen	Catalogus	Digitale oplossing

Verwijzing naar voorschrift	Beschrijving van voorschrift	Betrokken actoren	Processen op hoog niveau	Categorieën
<i>van software</i>	intellectuele-eigendomsrechten hebben, beschikbaar stelt voor hergebruik, stelt zij of het de software beschikbaar voor hergebruik in een catalogus die of register dat gekoppeld is aan de EU-OSS-catalogus.	Europese Commissie		
TITEL IV AUTONOMIE <i>Artikel 43 De EU-catalogus van opensourceoplossingen</i>	De Commissie verstrekt en onderhoudt een EU-catalogus van opensourceoplossingen (“EU-OSS-catalogus”) als gecentraliseerde catalogus om toegang te krijgen tot software die door entiteiten van de Unie en openbare lichamen beschikbaar wordt gesteld voor hergebruik. De EU-OSS-catalogus wordt gehost op het Interoperabel Europa-portaal. De Commissie neemt een besluit over het verzoek van een entiteit van de Unie die of openbaar lichaam dat eigenaar is van een catalogus of register of die een catalogus of register bijhoudt, om die catalogus of dat register te koppelen aan en toegankelijk te maken via de EU-OSS-catalogus.	Europese Commissie	Catalogus	Digitale oplossing

4.2. Gegevens

Korte beschrijving van de betrokken data

Soort gegevens	Verwijzing naar voorschrift(en)	Standaard en/of specificatie (indien van toepassing)
Nationale strategieën van de lidstaten	TITEL II ONDERZOEKS-, ONTWIKKELINGS- EN UITROLACTIVITEITEN VOOR HET CLOUD- EN AI-ECOSYSTEEM <i>Artikel 7 Nationale cloud- en AI-strategieën</i>	Minimale inhoudelijke vereisten voor de nationale strategieën.
Gegevens met betrekking tot aanvragen voor erkenning als strategisch project	TITEL III DATACENTRUMCAPACITEIT <i>Artikel 14 Aanwijzing van strategische datacentrumprojecten</i>	Verstreking van alle noodzakelijke en relevante informatie om aan te tonen dat het project aan de relevante criteria voldoet.
Statistieken en gegevens die nodig zijn voor de monitoring van de capaciteitskloof	TITEL III DATACENTRUMCAPACITEIT <i>Artikel 15 Monitoring van de capaciteitskloof</i>	n.v.t.
Gegevens in het kader van de indiening van aanvragen door dienstverleners die willen worden erkend als aanbieders van een Uniebetrouwbaarheidsniveau.	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	n.v.t.
EU-conformiteitsverklaring	TITEL IV AUTONOMIE <i>Artikel 19 Conformiteitszelfbeoordeling</i>	n.v.t.
Controlerapport ingediend voor erkenning en daarmee verband houdende uitwisselingen	TITEL IV AUTONOMIE <i>Artikel 20 Onafhankelijke controle</i> <i>Artikel 21 Inhoud en kwaliteit van controlebewijs</i>	Gegevenskwaliteit: voldoende volledig en betrouwbaar; minimuminhoud voor controles.

Gegevens over diensten die een erkenning krijgen	TITEL IV AUTONOMIE <i>Artikel 22 Centraal register van cloudcomputingdiensten</i>	Het centrale register bevat informatie over cloudcomputingdiensten die op grond van specifieke Uniebetrouwbaarheidsniveaus zijn erkend.
Kennisgeving van kennisneming van informatie of materiële verandering in de omstandigheden met betrekking tot de cloudcomputingdiensten die van invloed kan zijn op het controlerapport/controleadvies/erkenning en de daarmee verband houdende gegevensstromen	TITEL IV AUTONOMIE <i>Artikel 23 Transparantieplichtingen</i>	n.v.t.
Kennisgeving van regels en maatregelen inzake sancties	TITEL IV AUTONOMIE <i>Artikel 24 Sancties en schadevergoeding</i>	n.v.t.
Gegevens over de aangewezen nationale bevoegde autoriteiten	TITEL IV AUTONOMIE <i>Artikel 25 Nationale bevoegde autoriteiten</i>	n.v.t.
Gegevens die worden gebruikt in het kader van de samenwerking tussen nationale bevoegde autoriteiten	TITEL IV AUTONOMIE <i>Artikel 27 Wederzijdse bijstand</i>	n.v.t.
Gegevens die worden gebruikt in het kader van landsgrensoverschrijdende samenwerking	TITEL IV AUTONOMIE <i>Artikel 28 Landsgrensoverschrijdende samenwerking</i>	n.v.t.
Door de lidstaten uitgevoerde risicobeoordelingen	TITEL IV AUTONOMIE	n.v.t.

	<i>Artikel 29 Risicobeoordelingen</i>	
Ondersteunende informatie die door aanbieders aan de Commissie wordt verstrekt	TITEL IV AUTONOMIE <i>Artikel 29 Risicobeoordelingen</i>	n.v.t.
Gegevens met betrekking tot de monitoring van aanbestedingen voor innovatieve clouddiensten en AI-systemen	TITEL IV AUTONOMIE <i>Artikel 33 Innovatiegericht aanbesteden</i>	n.v.t.

Afstemming op Europese datastrategie

Toelichting hoe het voorschrift of de voorschriften zijn afgestemd op de Europese datastrategie

Het voorstel is in overeenstemming met de regels inzake het overstappen naar een andere dataverwerkingsdienst die zijn ingevoerd bij de dataverordening. Door overstappen mogelijk te maken en belangrijke bronnen van afhankelijkheid van één aanbieder weg te nemen, wil de dataverordening ervoor zorgen dat aanbieders van clouddiensten in de EU concurreren op kwaliteit, innovatie en prijs. Het doel is om cloudgebruikers in staat te stellen vrij te kiezen welke aanbieder het beste aan hun behoeften voldoet en het aanbod van verschillende aanbieders te combineren in een multicloudbenadering. De dataverordening bevat echter geen elementen om een concurrerender aanbod van clouddiensten in de EU vorm te geven of de toegang tot de markt door een diversere groep aanbieders van clouddiensten aan te moedigen. De dataverordening maakt de weg vrij voor een mogelijke vermindering van de afhankelijkheid van aanbieders van buiten de EU, maar legt niet de basis voor een meer soevereine en betrouwbare cloudcomputingsector in de EU. De bepalingen inzake overstappen naar andere clouddiensten en interoperabiliteit maken het voor gebruikers echter mogelijk om meer gebruik te maken van Europese cloudcomputingdiensten. De dataverordening maakt dit voorstel derhalve mogelijk.

Afstemming op eenmaligheidsbeginsel

Toelichting hoe het eenmaligheidsbeginsel in aanmerking is genomen en hoe is nagegaan of bestaande data kunnen worden hergebruikt

Het eenmaligheidsbeginsel is naar behoren in overweging genomen en wordt waar nodig systematisch gehandhaafd. Dit is in het bijzonder het geval voor:

- a) de statistieken en gegevens die nodig zijn voor de monitoring van de capaciteitskloof;
- b) de gegevens over diensten die een erkenning krijgen;
- c) aan de Commissie verstrekte informatie voor marktanalyse.

Toelichting hoe nieuw gecreëerde data vindbaar, toegankelijk, interoperabel en herbruikbaar zijn en aan hoge standaarden voldoen

Er worden digitale oplossingen aangeboden om de vindbaarheid, toegankelijkheid, interoperabiliteit en herbruikbaarheid van nieuw gecreëerde gegevens te waarborgen. Minimumeisen inzake inhoud zullen hoogwaardige normen voor de gegevens bevorderen.

Gegevensstromen

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
Nationale strategieën van de lidstaten	TITEL II ONDERZOEKS-, ONTWIKKELINGS- EN UITROLACTIVITEITEN VOOR HET CLOUD- EN AI-ECOSYSTEEM	Lidstaten	Europese Commissie	Binnen drie maanden na de goedkeuring van een nationale strategie	Per goedkeuring/herziening

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
	<i>Artikel 7 Nationale cloud- en AI-strategieën</i>				
Gegevens met betrekking tot aanvragen voor erkenning als strategisch project	TITEL III DATACENTRUMCAPACITEIT <i>Artikel 14 Aanwijzing van strategische datacentrumprojecten</i>	Aanvrager van de aanwijzing van een strategisch project	Europese Commissie	Aanvraag tijdens openbare oproepen tot het indienen van blijken van belangstelling	//
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Aanvragende aanbieder van cloudcomputingdiensten	Nationale bevoegde autoriteit van vestiging	Verzoek om diensten te verlenen aan entiteiten van de Unie en openbare lichamen	//
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: resultaat van	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Nationale bevoegde instantie	Aanvragende aanbieder van cloudcomputingdiensten	Conclusie met betrekking tot de eerste erkenning	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
het verzoek (afwijzing, verzoek om aanvullend bewijs, erkenning van de dienst van de aanbieder)					
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: verspreiding van de conclusie voor herziening	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Nationale bevoegde instantie	Alle bevoegde nationale instanties	Aanbieder van cloudcomputingdiensten die in kennis is gesteld van een erkenning	//
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: bezwaren	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Alle bevoegde nationale instanties	Nationale bevoegde instantie	De nationale bevoegde autoriteit heeft bezwaren tegen een conclusie van een nationale bevoegde autoriteit van vestiging	//
Gegevens in het kader van de indiening van	TITEL IV	Nationale bevoegde autoriteiten	Europese Commissie	Nationale bevoegde autoriteiten kunnen	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: naar de Commissie doorverwezen zaken	AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>			geen overeenstemming bereiken	
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: besluit van de Commissie inzake een doorverwezen zaak	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Europese Commissie	Nationale bevoegde autoriteiten	Commissie neemt besluit over zaak wanneer de nationale bevoegde autoriteiten geen overeenstemming kunnen bereiken	//
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Nationale bevoegde autoriteiten	Europese Commissie	Nationale bevoegde autoriteiten besluiten gebruik te maken van hun recht op een verzoek om informatie	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
van de Unie en openbare lichamen: verzoek om informatie					
Gegevens in het kader van de indiening van verzoeken door aanbieders van cloudcomputingdiensten die diensten willen verlenen aan entiteiten van de Unie en openbare lichamen: antwoord op een verzoek om informatie	TITEL IV AUTONOMIE <i>Artikel 17 Erkenning van aanbieders van cloudcomputingdiensten</i>	Europese Commissie	Nationale bevoegde autoriteiten	Verzoek om informatie van nationale bevoegde autoriteiten ontvangen	//
EU-conformiteitsverklaring	TITEL IV AUTONOMIE <i>Artikel 19 Conformiteitszelfbeoordeling</i>	Aanbieders van cloudcomputingdiensten	In handen van de overheid	Zelfevaluatie gebruikt	//
Controlerapport ingediend ter validering en daarmee verband houdende uitwisselingen: voor de controle vereiste informatie	TITEL IV AUTONOMIE <i>Artikel 20 Onafhankelijke controle</i> <i>Artikel 21 Inhoud en</i>	Aanbieders van cloudcomputingdiensten	Controleorganisatie	Controle wordt uitgevoerd	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
	<i>kwaliteit van controlebewijs</i>				
Controlerapport ingediend ter validering en daarmee verband houdende uitwisselingen: controlerapporten	TITEL IV AUTONOMIE <i>Artikel 20 Onafhankelijke controle</i> <i>Artikel 21 Inhoud en kwaliteit van controlebewijs</i>	Aanbieders van cloudcomputingdiensten	Controleorganisatie en nationale bevoegde autoriteiten	Audit afgerond	//
Gegevens over diensten die een erkenning krijgen: Centraal register van cloudcomputingdiensten	TITEL IV AUTONOMIE <i>Artikel 22 Centraal register van cloudcomputingdiensten</i>	Verifiërende bevoegde nationale instantie	Centraal register van cloudcomputingdiensten (Europese Commissie)	Erkenning verleend	//
Gegevens over diensten die een erkenning krijgen: openbaar toegankelijke website van de Europese Commissie	TITEL IV AUTONOMIE <i>Artikel 22 Centraal register van cloudcomputingdiensten</i>	Europese Commissie Nationale bevoegde instantie van vestiging	In handen van de overheid	Erkenning verleend	//
Kennisgeving van kennisneming van informatie of materiële verandering in de omstandigheden met betrekking tot de cloudcomputingdiensten	TITEL IV AUTONOMIE <i>Artikel 23 Transparantieverplichtingen</i>	Aanbieders van cloudcomputingdiensten	Controleorganisatie, nationale bevoegde autoriteit Europese Commissie	Materiële voorwaarden veranderen aan de kant van de aanbieder	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
die van invloed kan zijn op het controlerapport/controlerapport en de daarmee verband houdende gegevensstromen: eerste kennisgeving					
Kennisgeving van kennisgeving van informatie of materiële verandering in de omstandigheden met betrekking tot de cloudcomputingdiensten die van invloed kan zijn op het controlerapport/controlerapport en de daarmee verband houdende gegevensstromen: kennisgeving van de wijziging van de uitkomst van de controle	TITEL IV AUTONOMIE <i>Artikel 23 Transparantieplichtingen</i>	Controleorganisatie	Nationale bevoegde autoriteiten (van vestiging en van andere lidstaten) Europese Commissie	Resultaat van de controle gewijzigd	//
Kennisgeving van regels en maatregelen inzake sancties	TITEL IV AUTONOMIE <i>Artikel 24 Sancties en</i>	Lidstaten	Europese Commissie	De lidstaten stellen het kader voor het opleggen van	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
	<i>schadevergoeding</i>			sancties vast/wijzigen dit kader.	
Gegevens over de aangewezen nationale bevoegde autoriteiten: kennisgeving door de lidstaten	TITEL IV AUTONOMIE <i>Artikel 25 Nationale bevoegde autoriteiten</i>	Lidstaten	Europese Commissie	Aangewezen nationale bevoegde autoriteiten (binnen een jaar na de datum van inwerkingtreding)	//
Gegevens over de aangewezen nationale bevoegde autoriteiten: gegevens in het openbaar register van autoriteiten	TITEL IV AUTONOMIE <i>Artikel 25 Nationale bevoegde autoriteiten</i>	Europese Commissie	In handen van de overheid	Aangewezen nationale bevoegde autoriteiten en kennisgeving aan de Commissie	//
Gegevens die worden gebruikt in het kader van de samenwerking tussen nationale bevoegde autoriteiten: informatie-uitwisseling	TITEL IV AUTONOMIE <i>Artikel 27 Wederzijdse bijstand</i>	Nationale bevoegde autoriteiten	Nationale bevoegde autoriteiten	Samenwerking (uitwisseling van informatie) tussen nationale bevoegde autoriteiten nodig	//
Gegevens die worden gebruikt in het kader van de samenwerking tussen nationale bevoegde autoriteiten: verzoeken om bijstand (en	TITEL IV AUTONOMIE <i>Artikel 27 Wederzijdse bijstand</i>	Nationale bevoegde autoriteiten	Nationale bevoegde autoriteiten	Noodzakelijk geachte bijstand	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
antwoorden op dergelijke verzoeken)					
Gegevens die worden gebruikt in het kader van landsgrensoverschrijdende samenwerking: verzoek om beoordeling — vermoeden van niet-naleving	TITEL IV AUTONOMIE <i>Artikel 28</i> <i>Landsgrensoverschrijdende samenwerking</i>	Nationale bevoegde autoriteiten van bestemming van een dienst	Nationale bevoegde autoriteiten van herkomst van een dienst	Vermoedens van niet-naleving die aanleiding geven tot een verzoek om bijstand	//
Gegevens die worden gebruikt in het kader van landsgrensoverschrijdende samenwerking: Commissie op de hoogte gebracht van vermoedens van niet-naleving	TITEL IV AUTONOMIE <i>Artikel 28</i> <i>Landsgrensoverschrijdende samenwerking</i>	Nationale bevoegde autoriteiten van bestemming van een dienst	Europese Commissie	Een bevoegde autoriteit besluit de bevoegde autoriteit van vestiging om informatie te verzoeken om vermoedens van niet-naleving te beoordelen	//
Gegevens die worden gebruikt in het kader van landsgrensoverschrijdende samenwerking: verzoek om beoordeling — vermoeden van niet-naleving (Commissie)	TITEL IV AUTONOMIE <i>Artikel 28</i> <i>Landsgrensoverschrijdende samenwerking</i>	Nationale bevoegde autoriteiten van herkomst van een dienst	Europese Commissie Nationale bevoegde autoriteiten	Vermoeden van niet-naleving door andere bevoegde autoriteiten of de Commissie	//
Gegevens die worden gebruikt in het kader van	TITEL IV	Bevoegde autoriteiten van	Verzoekers Europese	Binnen twee maanden na	//

Soort gegevens	Verwijzing naar voorschrift(en)	Actoren die gegevens verstrekken	Actoren die gegevens ontvangen	Aanleiding voor uitwisseling van gegevens	Frequentie (indien van toepassing)
landsgrensoverschrijdende samenwerking: resultaat van een verzoek om beoordeling — vermoeden van niet-naleving	AUTONOMIE <i>Artikel 28 Landsgrensoverschrijdende samenwerking</i>	herkomst	Commissie	indiening van het verzoek	
Door de lidstaten uitgevoerde risicobeoordelingen	TITEL IV AUTONOMIE <i>Artikel 29 Risicobeoordelingen</i>	Lidstaten	Europese Commissie	Risicobeoordeling binnen een jaar na de inwerkingtreding	Halfjaarlijks
Ter informatie aan de Commissie verstrekte informatie	TITEL IV AUTONOMIE <i>Artikel 29 Risicobeoordelingen</i>	Aanbieders van clouddiensten	Europese Commissie	//	//
Gegevens met betrekking tot de monitoring van aanbestedingen voor innovatieve clouddiensten en AI-systemen	TITEL IV AUTONOMIE <i>Artikel 33 Monitoring van aanbesteding voor innovatie op het gebied van cloud en AI</i>	Lidstaten	Europese Commissie	//	Jaarlijks

4.3. Digitale oplossingen

Register van erkende cloudcomputingdiensten

Digitale en/of sectorale beleidsmaatregelen (indien van toepassing)	Uitleg over afstemming
<i>AI-verordening</i>	Niet van toepassing.
<i>EU-kader voor cyberbeveiliging</i>	Het register volgt de beste praktijken van de Commissie op het gebied van cyberbeveiliging
<i>eIDAS</i>	Het register zal, voor zover relevant, het eIDAS-kader hergebruiken.
<i>Eén digitale toegangspoort en IMI</i>	Niet van toepassing.
<i>Andere (bv. verordening Interoperabel Europa)</i>	De noodzaak van een andere interoperabiliteitsbeoordeling in het kader van de verordening Interoperabel Europa (Verordening (EU) 2024/903) zal worden geëvalueerd zodra de operationele details voor het register van erkende cloudcomputingdiensten beschikbaar zijn.

EuroCloud-platform

Digitale en/of sectorale beleidsmaatregelen (indien van toepassing)	Uitleg over afstemming
<i>AI-verordening</i>	Niet van toepassing.
<i>EU-kader voor cyberbeveiliging</i>	Het platform moet mechanismen voor veilige toegang en incidentenbeheer omvatten, zoals gedeeld identiteitsbeheer, instrumenten voor wederzijdse authenticatie en instrumenten voor het melden van incidenten. Het platform

	volgt de beste praktijken van de Commissie op het gebied van cyberbeveiliging.
<i>eIDAS</i>	Dit zal in een later stadium door de Commissie worden vastgesteld.
<i>Eén digitale toegangspoort en IMI</i>	Niet van toepassing.
<i>Andere (bv. verordening Interoperabel Europa)</i>	De noodzaak van een andere interoperabiliteitsbeoordeling in het kader van de verordening Interoperabel Europa (Verordening (EU) 2024/903) wordt geëvalueerd zodra de operationele details voor het EuroCloud-platform beschikbaar zijn.

Gemeenschappelijk aanbestedingsplatform

Digitale en/of sectorale beleidsmaatregelen (indien van toepassing)	Uitleg over afstemming
<i>AI-verordening</i>	Niet van toepassing.
<i>EU-kader voor cyberbeveiliging</i>	Het platform volgt de beste praktijken van de Commissie op het gebied van cyberbeveiliging.
<i>eIDAS</i>	Dit zal in een later stadium door de Commissie worden vastgesteld.
<i>Eén digitale toegangspoort en IMI</i>	Niet van toepassing.
<i>Andere (bv. verordening Interoperabel Europa)</i>	Niet van toepassing.

Catalogus of register van herbruikbare software die verbonden is met de EU-OSS-catalogus

Digitale en/of sectorale beleidsmaatregelen (indien van toepassing)	Uitleg over afstemming
<i>AI-verordening</i>	Niet van toepassing.
<i>EU-kader voor cyberbeveiliging</i>	Het platform volgt de beste praktijken van de Commissie op het gebied van cyberbeveiliging.
<i>eIDAS</i>	Het register zal, voor zover relevant, het eIDAS-kader hergebruiken.
<i>Eén digitale toegangspoort en IMI</i>	Niet van toepassing.
<i>Andere (bv. verordening Interoperabel Europa)</i>	Niet van toepassing.

De EU-catalogus van opensourceoplossingen

Digitale en/of sectorale beleidsmaatregelen (indien van toepassing)	Uitleg over afstemming
<i>AI-verordening</i>	Niet van toepassing.
<i>EU-kader voor cyberbeveiliging</i>	Het platform volgt de beste praktijken van de Commissie op het gebied van cyberbeveiliging.
<i>eIDAS</i>	In de catalogus zal, voor zover relevant, het eIDAS-kader worden hergebruikt.
<i>Eén digitale toegangspoort en IMI</i>	Niet van toepassing.

Andere (bv. verordening Interoperabel Europa)	Artikel 4 van de verordening Interoperabel Europa (Verordening (EU) 2024/903) schrijft het delen en hergebruiken van interoperabiliteitsoplossingen tussen entiteiten van de Unie en openbare lichamen voor. De EU-catalogus van opensourceoplossingen voldoet aan deze eis.
--	--

4.4. Interoperabiliteitsbeoordeling

Digitale overheidsdienst of categorie digitale overheidsdiensten	Beschrijving	Verwijzing naar voorschrift(en)	Interoperabel Europa-oplossing(en)	Andere interoperabiliteitsoplossing(en)
EU-register van erkende soevereine diensten	Een specifiek EU-register van cloudcomputingdiensten die erkenning hebben gekregen. Op te richten en in stand te houden door de Commissie. De nationale bevoegde autoriteiten registreren de betrokken diensten in dit register.	TITEL IV AUTONOMIE <i>Artikel 22 Centraal register van cloudcomputingdiensten</i>	//	N.v.t.
Federatie EuroCloud	Bij artikel 34 wordt de Europese cloudfederatie voor de publieke sector (Federatie EuroCloud) opgericht. De Federatie EuroCloud moet nationale cloudinitiatieven samenbrengen die zeer betrouwbare en veilige cloudcapaciteiten van de overheidssector bieden en het delen van dergelijke capaciteiten tussen entiteiten van de Unie en openbare	TITEL IV AUTONOMIE <i>Artikel 34 Oprichting van de Europese cloudfederatie voor de publieke sector</i>	N.v.t.	N.v.t.

	lichamen vergemakkelijken. Dit moet gebeuren via een platform dat toegankelijk is voor alle leden van de federatie — het EuroCloud-platform.			
--	--	--	--	--

Effect van het voorschrift/de voorschriften op landsgrensoverschrijdende interoperabiliteit per digitale overheidsdienst

EU-register van erkende soevereine diensten

Beoordeling	Maatregel(en)	Mogelijke resterende belemmeringen (indien van toepassing)
Afstemming op bestaand digitaal en sectoraal beleid Vermeld het toepasselijke digitale en sectorale beleid dat is vastgesteld.	Bij de uitvoering van het Unieregister van erkende soevereine diensten zal zoveel mogelijk rekening worden gehouden met het bestaande beleid en de daaruit voortvloeiende bouwstenen.	
Organisatorische maatregelen voor een vlotte landsgrensoverschrijdende verlening van digitale overheidsdiensten Vermeld de geplande governancemaatregelen.	De Europese Commissie is belast met het opzetten en onderhouden van het register. De controlerende nationale autoriteit is verantwoordelijk voor het uploaden van de relevante gegevens in het register.	De organisatorische maatregelen moeten in een later stadium door de Commissie worden uitgewerkt.
Maatregelen om te zorgen voor een gedeeld begrip van de data Geef een lijst met dergelijke maatregelen.	Semantische maatregelen worden in een later stadium door de Commissie vastgesteld.	
Gebruik van gezamenlijk	Technische maatregelen worden in een later stadium	

overeengekomen open technische specificaties en normen Geef een lijst met dergelijke maatregelen.	door de Commissie vastgesteld.	
--	--------------------------------	--

Federatie EuroCloud

Beoordeling	Maatregel(en)	Mogelijke resterende belemmeringen (indien van toepassing)
Afstemming op bestaand digitaal en sectoraal beleid Vermeld het toepasselijke digitale en sectorale beleid dat is vastgesteld.	Bij de uitvoering van de Federatie EuroCloud wordt zoveel mogelijk rekening gehouden met het bestaande beleid en de daaruit voortvloeiende bouwstenen. Meer bepaald: NIS2 voor cyberbeveiliging, Simpl, gegevensruimten.	N.v.t.
Organisatorische maatregelen voor een vlotte landsgrensoverschrijdende verlening van digitale overheidsdiensten Vermeld de geplande governancemaatregelen.	De gedetailleerde governance van het EuroCloud-platform wordt via secundaire wetgeving geregeld.	N.v.t.
Maatregelen om te zorgen voor een gedeeld begrip van de data Geef een lijst met dergelijke	Semantische maatregelen worden in een later stadium door de Commissie vastgesteld.	N.v.t.

maatregelen.		
Gebruik van gezamenlijk overeengekomen open technische specificaties en normen Geef een lijst met dergelijke maatregelen.	Technische maatregelen worden in een later stadium door de Commissie vastgesteld.	N.v.t.

4.5. Maatregelen ter ondersteuning van de digitale uitvoering

Beschrijving van de maatregel	Verwijzing naar voorschrift(en)	Rol van de Commissie	Te betrekken actoren	Verwacht tijdschema
De Commissie is bevoegd uitvoeringshandelingen vast te stellen tot nadere bepaling van i) de technische, operationele en organisatorische maatregelen en ii) de procedure voor deelname aan de Federatie EuroCloud als bedoeld in artikel 40, lid 2.	Artikel 40, artikel 41	Opstellen van een of meer uitvoeringshandelingen	Europese Commissie Deelnemende lidstaten	Nog te bepalen



Brussel, 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

BIJLAGEN

bij

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

**tot vaststelling van een kader van maatregelen ter versterking van het Europese cloud-
en AI-ecosysteem (verordening cloud- en AI-ontwikkeling)**

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

BIJLAGE I

GROTE UITDAGINGEN

1. Grote uitdaging 1: milieuduurzaamheid, prestaties en beveiliging van de datacentra van de Unie

Het testen en uitrollen van technologieën voor datacentra in de hele Unie om de modernste stand van zaken op het gebied van energie- en hulpbronnefficiëntie te overtreffen.

Dit omvat het bereiken van een lagere PUE-waarde (*Power Usage Effectiveness*, oftewel doeltreffendheid stroomverbruik) en het mogelijk maken van aanzienlijk hogere benuttingsgraden van servers. Enkele voorbeelden:

- (1) ***Verlaging van het gemiddelde van de doeltreffendheid stroomverbruik (PUE):*** de milieuduurzaamheid en prestaties van de cloud- en edge-datacentra van de Unie verbeteren tot een gemiddelde PUE-waarde van 1,15 in de hele Unie. De belangrijkste aandachtsgebieden zijn onder meer het mogelijk maken van de ontwikkeling van:
 - (a) geavanceerde technologieën voor energie-efficiëntie van datacentra, zoals koeling en terugwinning van afvalwarmte;
 - (b) kwantumcomputingtechnologieën voor cloud- en computerinfrastructuuractiviteiten;
 - (c) netintegratie en geavanceerde energiebeheersystemen;
 - (d) proeflijnen voor de validatie van energie-efficiënte technologieën van de volgende generatie op operationele schaal;
- (2) ***Verhoging van de gemiddelde serverbenuttingsgraad van datacentra:*** het verhogen van de gemiddelde benuttingsgraad van servers in alle datacentra van de Unie tot 50 %, door bijvoorbeeld AI-aangedreven technologieën te integreren voor dynamisch beheer van het servergebruik, beheer en planning van runtime workloads of voor het afwegen van benutting, energiekosten, thermische beperkingen en latentievereisten;
- (3) ***Verbetering van de beveiliging en veerkracht van datacentra:*** het verbeteren van de beveiliging en veerkracht van de waardeketen en levering van datacentra door de integratie van halfgeleider technologieën en kwantumtechnologieën die in de Unie zijn ontworpen en vervaardigd, en door hun weerstand tegen fysieke en cyberbeveiligingsdreigingen, zoals gerichte aanvallen, te verbeteren.

2. Grote uitdaging 2: cloudstacks

Het bouwen van end-to-end hardware- en software-cloudstacks, zoals AI-instrumenten, infrastructuur, diensten en beheerslagen om de kritieke capaciteitstekorten van de Unie te dichten.

Dit omvat de bouw van AI-servers die gebruikmaken van halfgeleiders en kwantumtechnologieën die in de Unie zijn ontworpen en vervaardigd voor gedistribueerde en gedecentraliseerde cloud- en edgecomputing voor AI.

Proefprogramma's kunnen helpen om te laten zien wat de capaciteit is van de Europese opencloudstacks in strategisch belangrijke sectoren.

3. Grote uitdaging 3: grensverleggende AI

Het ontwikkelen van multimodale grensverleggende AI-modellen en -systemen van de volgende generatie en baanbrekende nieuwe capaciteiten.

De nadruk zal liggen op het architectonische ontwerp en de ontwikkeling van multimodale modellen en systemen van de volgende generatie die de grenzen van de huidige algoritmische capaciteiten verleggen om betere prestaties te behalen op het gebied van geavanceerd redeneren, intermodaal inzicht en de capaciteiten van agenten; onderzoek naar nieuwe benaderingen van modelefficiëntie, cognitieve modellering en alternatieve rekenstructuren enz.

Mogelijke toepassingen zijn fundamentele wetenschap, zoals wetenschappelijke ontdekkingen en interpretatie van complexe gegevens, en de ontwikkeling van wereldmodellen voor verbeterde redenering en simulaties van geautomatiseerd beheer en planning.

4. Grote uitdaging 4: fysieke AI

Het ontwikkelen van geavanceerde fysieke AI-modellen en -systemen die autonoom en veilig werken en robuuste manipulatie- en navigatieprocessen in ongestructureerde omgevingen leveren.

De nadruk zal liggen op het gezamenlijk ontwerpen van software en de onderliggende hardware-architecturen en op het combineren van grensverleggende AI-technieken met wereldmodellen ter ondersteuning van fysieke redenering, om zo robuuste manipulatie-, navigatie- en interactiecapaciteiten te leveren die minimaal menselijk toezicht vereisen.

Mogelijke toepassingen zijn autonome robots, industriële systemen en drones voor toepassingen in dynamische reële omgevingen.

5. Grote uitdaging 5: AI voor industriële doeleinden

Het versnellen van de ontwikkeling en toepassing van Europese AI voor industriële doeleinden in de strategische sectoren van de Unie.

De nadruk zal liggen op de ontwikkeling van Europese industriële AI-modellen en systemen waarmee hoogwaardige industriële toepassingen mogelijk worden. Dergelijke modellen en systemen moeten kunnen worden aangepast aan sectorspecifieke gebruikssituaties en moeten veilig kunnen worden uitgerold.

Bij de initiatieven die in het kader van deze grote uitdaging worden gelanceerd, moet gebruik worden gemaakt van gespecialiseerde computermiddelen en de testfaciliteiten die nodig zijn om AI-systemen in reële omgevingen te valideren alvorens de grootschalige uitrol en toepassing ervan te ondersteunen, ook op regionaal en lokaal niveau.

In de automobielsector kunnen die initiatieven de ontwikkeling en uitrol van innovatieve softwareplatforms en AI-modellen voor geautomatiseerd rijden vergemakkelijken, terwijl zij op het gebied van de productie de ontwikkeling van gespecialiseerde modellen mogelijk kunnen maken die productieprocessen optimaliseren. Andere strategische sectoren die baat kunnen hebben bij AI voor industriële doeleinden zijn de gezondheidszorg, de energiesector, agrovoeding en defensie.

6. Grote uitdaging 6: coöperatieve Europese industriële modellen

Het ontwikkelen van coöperatieve Europese industriële AI-modellen en systemen voor strategische sectoren door industriële samenwerking op Europese schaal mogelijk te maken zonder commercieel gevoelige gegevens tussen deelnemers te delen.

De nadruk zal liggen op geavanceerde technologieën ter bescherming van de vertrouwelijkheid. Deze mechanismen omvatten gefedereerde en gedecentraliseerde benaderingen voor training, waarbij algoritmen op gegevens worden toegepast in plaats van dat gegevens centraal worden uitgewisseld; beveiligde uitvoeringsomgevingen, op versleuteling gebaseerde verwerking, anonimiserings- en pseudonimiseringstechnieken,

compartimentering van toegang en bescherming tegen de extractie van commercieel gevoelige informatie uit getrainde modellen.

Strategische sectoren die kunnen profiteren van coöperatieve Europese industriële AI-modellen en -systemen zijn onder meer de lucht- en ruimtevaart, de farmaceutische sector, cyberbeveiliging, mobiliteit, autonome voertuigen en drones, energie en defensie.

7. Grote uitdaging 7: platform voor AI-agenten

Het ontwikkelen van een Europees kader voor de orkestratie van AI-agenten, dat de essentiële middleware biedt voor de veerkrachtige en veilige inzet van autonome agenten op grote schaal.

De nadruk zal liggen op i) het verkennen van innovatieve technologische paradigma's die het mogelijk maken dat meerdere AI-agenten doeltreffend kunnen samenwerken, waarbij de capaciteiten van opzichzelfstaande systemen worden overtroffen maar nog wel strenge veiligheidsnormen gelden; en ii) de oprichting van veerkrachtige, cloudgebaseerde open platforms voor het grootschalige beheer van AI-agenten.

Mogelijke toepassingen zijn gezondheidszorg (zoals ondersteuning van klinische besluitvorming en coördinatie van onderzoek), cyberbeveiliging (zoals het opsporen van en reageren op dreigingen) en fundamentele wetenschap.

8. Grote uitdaging 8: AI voor de publieke sector

Het ontwikkelen van AI-modellen en -systemen op basis van hoogwaardige gegevens uit de publieke sector die gericht zijn op kritieke domeinen (zoals gezondheidszorg, openbaar bestuur, recht en crisisbeheersing, alsook overheidsdiensten)

De nadruk zal liggen op oplossingen voor overheidsdiensten die naar verwachting een groot positief effect zullen hebben op de meest kritieke overheidsdiensten en die worden gedeeld tussen de verschillende niveaus van de overheidsorganisaties.

Een van de doelstellingen is het delen van gegevens en de ontwikkeling van grensverleggende modellen tussen nationale overheidsdiensten mogelijk te maken om de impact op de overheidsdiensten van de Unie als geheel te vergroten, ook op gebieden waar gevoelige gegevens worden verwerkt. Kaders ter bescherming van de privacy (zoals gefedereerd leren en het genereren van zeer getrouwe synthetische gegevens), die het mogelijk maken modellen te trainen zonder de vertrouwelijkheid van onderliggende datasets in gevaar te brengen, en maatregelen om de brede toepassing van deze modellen te versnellen, ook op regionaal en lokaal niveau, zullen ook bijdragen tot de verwezenlijking van deze doelstelling.

BIJLAGE II

CRITERIA VOOR UNIEBETROUWBAARHEIDSNIVEAUS

Deze bijlage bevat de criteria waaraan aanbieders van cloudcomputingdiensten en hun cloudcomputingdiensten moeten voldoen om te worden erkend als aanbieders van diensten op Uniebetrouwbaarheidsniveaus 1, 2, 3 en 4. Voor de toepassing van de criteria ten aanzien van Uniebetrouwbaarheidsniveaus 1, 2, 3 en 4 valt “software” in de zin van Verordening (EU) 2024/2847, artikel 3, punt 4), binnen het toepassingsgebied van deze bijlage en bijlage III bij deze verordening. “Hardware” valt, in de zin van artikel 3, punt 5), van Verordening (EU) 2024/2847, buiten het toepassingsgebied ervan.

1. Uniebetrouwbaarheidsniveau 1

1.1. Voor Uniebetrouwbaarheidsniveau 1 moeten aanbieders van cloudcomputingdiensten aan elk van de volgende criteria voldoen:

- (a) de aanbieder van cloudcomputingdiensten is gevestigd in de Unie;
- (b) de infrastructuur en activa van de aanbieder van cloudcomputingdiensten, waaronder die van onderaannemers die betrokken zijn bij de dienstverlening, bevinden zich in de Unie, tenzij het openbaar lichaam uitdrukkelijk anders voorschrijft;
- (c) de klantgegevens, inclusief metagegevens en telemetriegegevens, die worden verwerkt, opgeslagen en overgedragen door de aanbieder van cloudcomputingdiensten en door de onderaannemers die betrokken zijn bij de dienstverlening, blijven uitsluitend en te allen tijde, ook vóór, tijdens of na de configuratie of het gebruik van de dienst, binnen de Unie, tenzij het openbaar lichaam uitdrukkelijk anders voorschrijft;
- (d) wanneer de aanbieder van cloudcomputingdiensten de technische en operationele ondersteuning of bijstand, zoals eventuele latere onderaanbestedingsovereenkomsten, uitbesteedt aan derde dienstverleners buiten de Unie, worden de nodige juridische, technische en organisatorische maatregelen getroffen om de traceerbaarheid, beveiliging en governance van die activiteiten te waarborgen en te garanderen dat die activiteiten de operationele autonomie van de aanbieder van cloudcomputingdiensten op geen enkele wijze in gevaar brengt;
- (e) de aanbieder van cloudcomputingdiensten toont aan dat de dienst voldoet aan de modernste cyberbeveiligingsnormen;
- (f) de aanbieder van cloudcomputingdiensten zorgt voor volledige transparantie over het inzetten van onderaannemers. De aanbieder van cloudcomputingdiensten onderwerpt onderaannemers aan zorgvuldigheidsprocedures, contractuele verplichtingen en doorlopend toezicht om aan de wettelijke verplichtingen van de Unie te voldoen;
- (g) wanneer de aanbieder van cloudcomputingdiensten onder zeggenschap staat van een derde land of een in een derde land gevestigde juridische entiteit, garandeert de aanbieder van cloudcomputingdiensten, middels onafhankelijke bronnen, dat er in dat derde land geen wetgeving is en praktijken gelden die de aanbieder van cloudcomputingdiensten verplichten informatie over kwetsbaarheden in software te melden aan de autoriteiten van dat derde land voordat bekend is dat die kwetsbaarheden zijn uitgebuit.

1.2. Voor Uniebetrouwbaarheidsniveau 1 moeten de in de eerste alinea bedoelde onderaannemers derden zijn die een directe contractuele relatie hebben met de

aanbieder van cloudcomputingdiensten en die bijdragen tot de verlening en levering van de cloudcomputingdienst.

2. Uniebetrouwbaarheidsniveau 2

2.1. Voor Uniebetrouwbaarheidsniveau 2 moeten aanbieders van cloudcomputingdiensten aan elk van de volgende criteria voldoen:

- (a) de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst zijn gevestigd in de Unie;
- (b) de infrastructuur, de activa en het personeel van de gecontroleerde aanbieder, inclusief die van de onderaannemers die betrokken zijn bij de dienstverlening, bevinden zich in de Unie;
- (c) de klantgegevens, inclusief metagegevens en telemetriegegevens, die worden verwerkt, opgeslagen en overgedragen door de gecontroleerde aanbieder en door de onderaannemers die betrokken zijn bij de dienstverlening, blijven uitsluitend en te allen tijde, ook vóór, tijdens of na de configuratie of het gebruik van de dienst, binnen de Unie, tenzij het openbaar lichaam uitdrukkelijk anders voorschrijft;
- (d) indien het openbaar lichaam bepaalt dat aanvullende screening van het personeel en voorschriften inzake EU-burgerschap nodig zijn, moet de gecontroleerde aanbieder ervoor zorgen dat er personeel beschikbaar is dat aan die vereisten voldoet;
- (e) de gecontroleerde dienst verkrijgt een Europees cyberbeveiligingscertificaat met ten minste het zekerheidsniveau “substantieel” in het kader van een Europese cyberbeveiligingscertificeringsregeling voor cloudcomputingdiensten die op grond van Verordening (EU) 2019/881 moet worden vastgesteld, op voorwaarde dat een dergelijke regeling op grond van die verordening is vastgesteld en beschikbaar is voor aanbieders van cloudcomputingdiensten. Totdat een dergelijke regeling is vastgesteld, zijn nationale regelingen voor cyberbeveiligingscertificering van toepassing, voor zover deze bestaan. Indien er geen regelingen voor cyberbeveiligingscertificering op Unie- of nationaal niveau bestaan, moet de gecontroleerde aanbieder aantonen dat de dienst voldoet aan de hoogste cyberbeveiligingsnormen uit hoofde van het toepasselijke Unierecht;
- (f) de gegevens die door het gebruik van de gecontroleerde dienst worden gegenereerd, worden niet gebruikt voor het trainen of verfijnen van AI-systemen die door een derde land of een in een derde land gevestigde juridische entiteit worden geëxploiteerd, en worden in geen geval naar buiten de Unie doorgegeven;
- (g) indien de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst onder zeggenschap staan van een derde land of een in een derde land gevestigde juridische entiteit, tonen zij aan dat de nodige juridische, technische en organisatorische maatregelen zijn getroffen om ervoor te zorgen dat:
 - i. de zeggenschap van het derde land of de in een derde land gevestigde juridische entiteit over de gecontroleerde aanbieder niet zodanig wordt uitgeoefend dat het vermogen van de aanbieder om de dienst uit te voeren en te verlenen wordt belemmerd of beperkt, dat beperkingen worden opgelegd aan de voor de dienstverlening benodigde infrastructuur, activa en personeel, of dat de capaciteiten en normen die nodig zijn om de gecontroleerde dienst uit te voeren, worden ondermijnd;

- ii. de toegang van een derde land of van een in een derde land gevestigde juridische entiteit tot klantgegevens wordt verhinderd;
 - iii. de mogelijkheid van verstoring van de continuïteit van de dienstverlening en/of de verslechtering van de kwaliteit van de dienstverlening door een derde land of een in een derde land gevestigde juridische entiteit wordt voorkomen;
 - iv. de zeggenschap van het derde land of de in een derde land gevestigde juridische entiteit over de gecontroleerde aanbieder niet wordt uitgeoefend op een wijze die de gecontroleerde aanbieder verplicht beperkende maatregelen zoals sanctieregelingen, embargo's of gelijkwaardige wettelijke of bestuursrechtelijke maatregelen van een derde land uit te voeren, te handhaven of na te leven, tenzij dergelijke maatregelen rechtmatig zijn uit hoofde van het nationale recht van de lidstaten of het Unierecht;
- (h) de technische en operationele ondersteuning of bijstand in verband met de gecontroleerde dienst, inclusief latere onderaannestedingsregelingen, wordt uitsluitend binnen de Unie geïnitieerd en uitgevoerd;
- (i) de gecontroleerde aanbieder toont aan dat de volgende maatregelen voor de toeleveringsketen van software zijn getroffen:
- i. een volledige en actuele softwarestuklijst, zoals gedefinieerd in artikel 3, punt 39), van Verordening (EU) 2024/2847, en een lijst van vastgestelde afhankelijkheden die relevant zijn voor de verlening van de dienst, worden gedocumenteerd en ter beschikking gesteld van de controleorganisatie;
 - ii. wanneer softwarecomponenten zoals gedefinieerd in artikel 3, punt 6), van Verordening (EU) 2024/2847 of producten worden geleverd, eigendom zijn van en er een vergunning voor is gekregen van een in een derde land gevestigde juridische entiteit, worden er controles uitgevoerd en gedocumenteerd om functies op afstand te blokkeren die een apparaat, systeem of software wezenlijk zouden kunnen manipuleren of verstoren (ook tijdens updates) en om ervoor te zorgen dat de veiligheidsrelevante componenten van softwarefabrikanten uit derde landen, zoals gedefinieerd in artikel 3, punt 13), van Verordening (EU) 2024/2847, worden onderworpen aan controles van de broncode en over een gedocumenteerd migratieplan beschikken indien de verkoper failliet gaat of een derde land beperkingen oplegt;
 - iii. wanneer de aanbieder van cloudcomputingdiensten onder zeggenschap staat van een derde land of een in een derde land gevestigde juridische entiteit, garandeert de aanbieder van cloudcomputingdiensten, middels onafhankelijke bronnen, dat er in dat derde land geen wetgeving is en praktijken gelden die de aanbieder van cloudcomputingdiensten verplichten informatie over kwetsbaarheden in software te melden aan de autoriteiten van dat derde land voordat bekend is dat die kwetsbaarheden zijn uitgebuit;
- (j) wanneer software die op grond van een opensourcelicentie is vrijgegeven, wordt gebruikt voor het verlenen van de dienst, toont de gecontroleerde aanbieder aan dat hij passende controles heeft ingevoerd en gedocumenteerd om het gebruik te voorkomen van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren;
- (k) voor zover de gecontroleerde aanbieder zijn diensten wereldwijd aanbiedt en een dochteronderneming in een derde land heeft, heeft de gecontroleerde aanbieder de nodige maatregelen getroffen om de doeltreffende juridische, technische en

organisatorische scheiding tussen de moederonderneming in de EU en een dergelijke dochteronderneming in een derde land te waarborgen en te handhaven.

- 2.2. Voor Uniebetrouwbaarheidsniveau 2 moeten de in de eerste alinea bedoelde onderaannemers onderaannemers zijn die derden zijn die een directe contractuele relatie hebben met de aanbieder van cloudcomputingdiensten en die bijdragen tot de verlening en levering van de cloudcomputingdienst.

3. Uniebetrouwbaarheidsniveau 3

- 3.1. Voor Uniebetrouwbaarheidsniveau 3 moeten aanbieders van cloudcomputingdiensten aan elk van de volgende criteria voldoen:

- (a) de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst zijn gevestigd in de Unie;
- (b) de infrastructuur, de activa en het personeel van de gecontroleerde aanbieder, inclusief die van de onderaannemers die betrokken zijn bij de dienstverlening, bevinden zich in de Unie;
- (c) de klantgegevens, inclusief metagegevens en telemetriegegevens, die worden verwerkt, opgeslagen en overgedragen door de gecontroleerde aanbieder en door de onderaannemers die betrokken zijn bij de dienstverlening, blijven uitsluitend en te allen tijde, ook vóór, tijdens of na de configuratie of het gebruik van de dienst, binnen de Unie, tenzij het openbaar lichaam uitdrukkelijk anders voorschrijft;
- (d) het personeel, inclusief het personeel van de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst, zijn EU-burgers en in voorkomend geval moet het personeel ook in het bezit zijn van de noodzakelijke nationale veiligheidsmachtiging die door een lidstaat is afgegeven wanneer zij gerubriceerde informatie, zoals gedefinieerd in artikel 2, punt 21), van Verordening (EU) 2021/697, behandelen;
- (e) de gecontroleerde dienst verkrijgt een Europees cyberbeveiligingscertificaat met ten minste het zekerheidsniveau “substantieel” in het kader van een Europese cyberbeveiligingscertificeringsregeling voor cloudcomputingdiensten die op grond van Verordening (EU) 2019/881 moet worden vastgesteld, op voorwaarde dat een dergelijke regeling op grond van die verordening is vastgesteld en beschikbaar is voor aanbieders van cloudcomputingdiensten. Totdat een dergelijke regeling is vastgesteld, zijn nationale regelingen voor cyberbeveiligingscertificering van toepassing, voor zover deze bestaan. Indien er geen regelingen voor cyberbeveiligingscertificering op Unie- of nationaal niveau bestaan, moet de gecontroleerde aanbieder aantonen dat de dienst voldoet aan de hoogste cyberbeveiligingsnormen uit hoofde van het toepasselijke Unierecht;
- (f) de gegevens die door het gebruik van de gecontroleerde dienst worden gegenereerd, worden niet gebruikt voor het trainen of verfijnen van AI-systemen die door een derde land of een in een derde land gevestigde juridische entiteit worden geëxploiteerd, en worden in geen geval naar buiten de Unie doorgegeven;
- (g) de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst staan niet onder zeggenschap van een derde land of een in een derde land gevestigde juridische entiteit. In afwijking van dit criterium kunnen een aanbieder van cloudcomputingdiensten en zijn onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst en die onder zeggenschap staan van een derde land of een in een derde land gevestigde juridische

entiteit, worden gecontroleerd voor Uniebetrouwbaarheidsniveau 3 indien de Commissie uit hoofde van artikel 19 een uitvoeringshandeling heeft vastgesteld. Indien de Commissie uit hoofde van artikel 19 een uitvoeringshandeling heeft vastgesteld, moeten de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst ook aantonen dat de nodige juridische, technische en organisatorische maatregelen zijn getroffen om ervoor te zorgen dat:

- i. de zeggenschap van het derde land of de in een derde land gevestigde juridische entiteit over de gecontroleerde aanbieder niet zodanig wordt uitgeoefend dat het vermogen van de aanbieder om de dienst uit te voeren en te verlenen wordt belemmerd of beperkt, dat beperkingen worden opgelegd aan de voor de dienstverlening benodigde infrastructuur, activa en personeel, of dat de capaciteiten en normen die nodig zijn om de gecontroleerde dienst uit te voeren, worden ondermijnd. De gecontroleerde aanbieder moet redelijke toegang tot de code mogelijk maken;
 - ii. de toegang van een derde land of van een in een derde land gevestigde juridische entiteit tot klantgegevens wordt verhinderd;
 - iii. de mogelijkheid van verstoring van de continuïteit van de dienstverlening en/of de verslechtering van de kwaliteit van de dienstverlening door een derde land of een in een derde land gevestigde juridische entiteit wordt voorkomen;
 - iv. de zeggenschap van het derde land of de in een derde land gevestigde juridische entiteit over de gecontroleerde aanbieder niet wordt uitgeoefend op een wijze die de gecontroleerde aanbieder verplicht beperkende maatregelen zoals sanctieregelingen, embargo's of gelijkwaardige wettelijke of bestuursrechtelijke maatregelen van een derde land uit te voeren, te handhaven of na te leven, tenzij dergelijke maatregelen rechtmatig zijn uit hoofde van het nationale recht van de lidstaten of het Unierecht;
- (h) de technische en operationele ondersteuning of bijstand in verband met de gecontroleerde dienst, inclusief latere onderaannestedingsregelingen, wordt uitsluitend binnen de Unie geïnitieerd en uitgevoerd, door personeel dat EU-burger is en door derden die niet onder zeggenschap staan van een derde land of een in een derde land gevestigde juridische entiteit;
- (i) de gecontroleerde aanbieder toont aan dat de volgende maatregelen voor de toeleveringsketen van software zijn getroffen:
- i. een volledige en actuele softwarestuklijst en een lijst van vastgestelde afhankelijkheden die relevant zijn voor de verlening van de dienst, worden gedocumenteerd en ter beschikking gesteld van de controleorganisatie;
 - ii. wanneer softwarecomponenten of producten worden geleverd, eigendom zijn van en er een vergunning voor is gekregen van een in een derde land gevestigde juridische entiteit, worden er controles uitgevoerd en gedocumenteerd om functies op afstand te blokkeren die een apparaat, systeem of software wezenlijk zouden kunnen manipuleren of verstoren (ook tijdens updates) en om ervoor te zorgen dat de veiligheidsrelevante componenten van softwarefabrikanten uit derde landen worden onderworpen aan controles van de broncode en over een gedocumenteerd migratieplan beschikken indien de verkoper failliet gaat of een derde land beperkingen oplegt;

- iii. wanneer de aanbieder van cloudcomputingdiensten onder zeggenschap staat van een derde land of een in een derde land gevestigde juridische entiteit, garandeert de aanbieder van cloudcomputingdiensten, middels onafhankelijke bronnen, dat er in dat derde land geen wetgeving is en praktijken gelden die de aanbieder van cloudcomputingdiensten verplichten informatie over kwetsbaarheden in software te melden aan de autoriteiten van dat derde land voordat bekend is dat die kwetsbaarheden zijn uitgebuit;
 - (j) wanneer software die op grond van een opensourcelicentie is vrijgegeven, wordt gebruikt voor het verlenen van de dienst, toont de gecontroleerde aanbieder aan dat hij passende controles heeft ingevoerd en gedocumenteerd om het gebruik te voorkomen van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren;
 - (k) voor zover de gecontroleerde aanbieder zijn diensten buiten de EU aanbiedt en een dochteronderneming in een derde land heeft, toont de gecontroleerde aanbieder aan de nodige maatregelen te hebben genomen om de doeltreffende juridische, technische en organisatorische scheiding tussen de moederonderneming in de EU en een dergelijke dochteronderneming in een derde land te waarborgen en te handhaven.
- 3.2. Voor Uniebetrouwbaarheidsniveau 3 moeten de in de eerste alinea bedoelde onderaannemers onderaannemers zijn die derden zijn die een directe contractuele relatie hebben met de aanbieder van cloudcomputingdiensten en die bijdragen tot de verlening en levering van de cloudcomputingdienst en die toegang nodig hebben tot gerubriceerde of gevoelige informatie, zoals gedefinieerd in artikel 2, punt 22), van Verordening (EU) 2021/697.

4. Uniebetrouwbaarheidsniveau 4

- 4.1. Voor Uniebetrouwbaarheidsniveau 4 moeten aanbieders van cloudcomputingdiensten aan elk van de volgende criteria voldoen:
- (a) de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst zijn gevestigd in de Unie;
 - (b) de infrastructuur, de activa en het personeel van de gecontroleerde aanbieder, inclusief die van de onderaannemers die betrokken zijn bij de dienstverlening, bevinden zich in de Unie;
 - (c) de klantgegevens, inclusief metagegevens en telemetriegegevens, die na een risicobeoordeling als gevoelig worden beschouwd en die worden verwerkt, opgeslagen en overgedragen door de gecontroleerde aanbieder en door de onderaannemers die betrokken zijn bij de dienstverlening, blijven uitsluitend en te allen tijde, ook vóór, tijdens of na de configuratie of het gebruik van de dienst, binnen de Unie;
 - (d) het personeel, inclusief het personeel van de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst, zijn EU-burgers en in voorkomend geval moet het personeel ook in het bezit zijn van de noodzakelijke nationale veiligheidsmachtiging die door een lidstaat is afgegeven wanneer zij gerubriceerde informatie behandelen;
 - (e) de gecontroleerde dienst verkrijgt een Europees cyberbeveiligingscertificaat met ten minste het zekerheidsniveau “hoog” in het kader van een Europese cyberbeveiligingscertificeringsregeling voor cloudcomputingdiensten die op grond van Verordening (EU) 2019/881 moet worden vastgesteld, op voorwaarde dat een

dergelijke regeling op grond van die verordening is vastgesteld en beschikbaar is voor aanbieders van cloudcomputingdiensten. Totdat een dergelijke regeling is vastgesteld, zijn nationale regelingen voor cyberbeveiligingscertificering van toepassing, voor zover deze bestaan. Indien er geen regelingen voor cyberbeveiligingscertificering op Unie- of nationaal niveau bestaan, moet de gecontroleerde aanbieder aantonen dat de dienst voldoet aan de hoogste cyberbeveiligingsnormen uit hoofde van het toepasselijke Unierecht;

- (f) de gegevens die door het gebruik van de gecontroleerde dienst worden gegenereerd, worden niet gebruikt voor het trainen of verfijnen van AI-systemen die door een derde land of een in een derde land gevestigde juridische entiteit worden geëxploiteerd, en worden in geen geval naar buiten de Unie doorgegeven;
 - (g) de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de gecontroleerde dienst staan niet onder zeggenschap van een derde land of een in een derde land gevestigde juridische entiteit;
 - (h) de technische en operationele ondersteuning of bijstand in verband met de gecontroleerde dienst, inclusief latere onderaannestedingsregelingen, wordt uitsluitend binnen de Unie geïnitieerd en uitgevoerd, door personeel dat EU-burger is en door derden die niet onder zeggenschap staan van een derde land of een in een derde land gevestigde juridische entiteit;
 - (i) de gecontroleerde aanbieder toont aan dat de volgende maatregelen voor de toeleveringsketen van software zijn getroffen:
 - i. een volledige en actuele softwarestuklijst en een lijst van vastgestelde afhankelijkheden die relevant zijn voor de verlening van de dienst, worden gedocumenteerd en ter beschikking gesteld van de controleorganisatie;
 - ii. er zijn maatregelen getroffen om doeltreffende zeggenschap over de softwarecomponenten of producten te behouden door aan te tonen dat een derde land of een in een derde land gevestigde juridische entiteit geen doeltreffende zeggenschap heeft of uitoefent over het ontwerp, de ontwikkeling, het onderhoud en de doorontwikkeling van die componenten of producten. Doeltreffende controle omvat het vermogen om wezenlijke invloed uit te oefenen op de technische doorontwikkeling, de onderhoudsprioriteiten, het herstel van de beveiliging en de continuïteit van de component op lange termijn;
 - (j) wanneer software die op grond van een opensourcelicentie is vrijgegeven, wordt gebruikt, toont de gecontroleerde aanbieder aan dat hij passende controles heeft ingevoerd en gedocumenteerd om het gebruik te voorkomen van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren;
 - (k) voor zover de gecontroleerde aanbieder zijn diensten buiten de EU aanbiedt en een dochteronderneming in een derde land heeft, toont de gecontroleerde aanbieder aan de nodige maatregelen te hebben genomen om de doeltreffende juridische, technische en organisatorische scheiding tussen de moederonderneming in de EU en een dergelijke dochteronderneming in een derde land te waarborgen en te handhaven.
- 4.2. Voor Uniebetrouwbaarheidsniveau 4 moeten de in de eerste alinea bedoelde onderaannemers onderaannemers zijn die derden zijn die een directe contractuele relatie hebben met de aanbieder van cloudcomputingdiensten, die bijdragen tot de

verlening en levering van de cloudcomputingdienst en die toegang nodig hebben tot gerubriceerde of gevoelige informatie om de diensten te kunnen verlenen.

BIJLAGE III

CONTROLEBEWIJS VOOR DE CONTROLEPROCEDURE

Controleorganisaties moeten de gecontroleerde aanbieder om het in deze bijlage vermelde controlebewijs verzoeken wanneer zij beoordelen of de gecontroleerde dienst voldoet aan de toepasselijke controlecriteria van bijlage II.

Deze bijlage is indicatief en houdt geen beperkingen in van het bewijsmateriaal dat door de controleorganisaties kan worden opgevraagd of in overweging kan worden genomen. Controleurs kunnen voor het uitvoeren van controles alle aanvullende informatie inwinnen die nodig is om een alomvattende en nauwkeurige beoordeling van de naleving te waarborgen. Hoewel het gevraagde bewijsmateriaal hetzelfde kan zijn, zullen de aspecten die moeten worden geanalyseerd, verschillen afhankelijk van de criteria voor het zekerheidsniveau en de striktheid ervan.

1. Controlecriterium A: vestiging in de Unie

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt a), van bijlage II vermelde controlecriterium beoordelen op basis van het volgende:

- (1) bewijsmateriaal waaruit blijkt dat de gecontroleerde aanbieder is opgericht naar het recht van een lidstaat in de Unie of anderszins is opgericht overeenkomstig het vennootschapsrecht van een lidstaat in de Unie;
- (2) bewijs dat de statutaire zetel, het hoofdkantoor en de hoofdvestiging van de gecontroleerde aanbieder in de Unie zijn gevestigd;
- (3) de controleorganisatie moet het toepasselijke rechtskader van de Unie van de gecontroleerde aanbieder verifiëren en nagaan of zijn vestiging reëel en duurzaam is, dan wel of de gecontroleerde aanbieder in plaats daarvan alleen kan worden aangemerkt als een aanbieder van buiten de EU die diensten aanbiedt in de Unie;
- (4) de controleorganisatie moet nagaan of de aanbieder wettelijk is opgericht in een lidstaat van de Unie. Bewijs hiervan kan bestaan uit, maar is niet beperkt tot, uittreksels uit het nationale handelsregister, documenten inzake fiscale woonplaats, bedrijfsvergunningen, btw-registratie, verificatie of de aanbieder is geregistreerd in het systeem van gekoppelde registers (BRIS) en het btw-informatie-uitwisselingssysteem (VIES);
- (5) de controleorganisatie moet de duurzame en doeltreffende aanwezigheid van de gecontroleerde aanbieder in de Unie verifiëren. De controleorganisatie moet daarom nagaan of:
 - (a) er fysieke kantoren of bedrijfsruimten in de EU aanwezig zijn (bv. door middel van huurovereenkomsten, rekeningen voor nutsvoorzieningen of eigendomsdocumenten);
 - (b) er vast personeel in de Unie is gevestigd en dat klantenondersteuningsactiviteiten in de Unie worden uitgevoerd (bv. door middel van arbeidsovereenkomsten, loonadministratie, arbeidstijdoverzichten van personeel);
 - (c) contractuele verrichtingen in de Unie worden uitgevoerd (bv. door middel van activiteitenbeheergegevens, gegevens over incidentenrapportage);

- (d) bank- en boekhoudfuncties uitsluitend in de Unie worden uitgeoefend (bv. door middel van financiële overzichten en wettelijke controlerapporten);
- (6) De controleorganisatie moet de aanwezigheid van vestigingseenheden of bijkantoren in de EU-lidstaten verifiëren (bv. door middel van leasecontracten, rekeningen van nutsvoorzieningen, eigendomsdocumenten, arbeidsovereenkomsten, arbeidstijdoverzichten, loonadministratie of aankooporders).

2. Controlecriterium B: locatie van infrastructuur, activa en personeel

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt b), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

(1) Locatie van de infrastructuur

- (a) Een lijst met relevante details over de locatie van de infrastructuur en de gegevensopslaglocaties die bij de verlening van de gecontroleerde dienst worden gebruikt. Deze lijst moet de precieze locatie (nummer, straat, stad, postcode en land) van de infrastructuur bevatten waaruit blijkt dat alle elementen voor de verlening van de gecontroleerde dienst zich binnen de Unie bevinden. Dit omvat de locatie voor primaire opslag, back-up, herstel na calamiteiten en opslag van logbestanden;
- (b) Elk ander bewijs dat de IT-infrastructuur zich in de Unie bevindt, zoals huurovereenkomsten, eigendomsakten, onderhoudscontracten, dienstverleningscontracten, toegangslags voor faciliteiten;
- (c) Netwerkdigrammen en architectuurdocumenten die aantonen dat de in de Unie gevestigde infrastructuur uitsluitend wordt gebruikt voor de opslag en verwerking van gegevens, waaronder back-up- en gekopieerde gegevens.

(2) Locatie van de activa

- (a) Een lijst en relevante gegevens van de activa die worden gebruikt bij het verlenen van de gecontroleerde dienst, zoals een register van activa;
- (b) Bewijs dat servers, apparatuur en operationele middelen zich in de Unie bevinden, zoals gegevens ter identificatie van de server en de locatie daarvan, aankoopfacturen, afleveringsbewijzen, licentieovereenkomsten, abonnementscontracten of facturen voor de aankoop van software of abonnementen, facturen met afleveringsbewijzen voor hardware;
- (c) Bewijs dat de capaciteit voor de dienstverlening in de Unie is gevestigd, zoals gebruiksgegevens, installatiegegevens, verslagen over de status van de dienst, configuratieverslagen, monitoringresultaten en administratieve logbestanden waaruit het gebruik van de dienst blijkt.

(3) Locatie van het personeel

- (a) Een lijst en relevante gegevens van het personeel dat betrokken is bij de verlening van de gecontroleerde dienst;
- (b) Bewijs dat het bij de verlening van de gecontroleerde dienst betrokken personeel zich in de Unie bevindt, inclusief arbeidsovereenkomsten, loonadministratie, arbeidstijdoverzichten, activiteitenoverzichten en organisatieschema's waaruit blijkt dat het in de Unie gevestigde personeel operationele verantwoordelijkheden heeft.

(4) Overwegingen met betrekking tot infrastructuur, activa en personeel

- (a) De controleorganisatie moet ook beoordelen of infrastructuur, activa of personeel:
 - i. klantgegevens opslaan, doorgeven, raadplegen, verwerken of anderszins behandelen;
 - ii. administratieve toegang tot, controle over, configuratie van of zichtbaarheid van klantgegevens verlenen, mogelijk maken of mogelijk zouden kunnen maken;
 - iii. indien zij gecompromitteerd worden, verkeerd worden geconfigureerd, onbeschikbaar worden gemaakt of worden verstoord, redelijkerwijs de verstoring of onbeschikbaarheid van de gecontroleerde dienst tot gevolg kunnen hebben.

NB: “Infrastructuur”: fysieke infrastructuur, zoals maar niet beperkt tot de infrastructuur van datacentra of colocaties en de netwerk-, koelings- en IT-systemen die het beheer van het datacentrum mogelijk maken.

“Activa”: hardware en software, zoals maar niet beperkt tot bibliotheken, het interne netwerk dat nodig is voor de communicatie van softwarecomponenten, cryptografisch materiaal dat de verlening van de cloudcomputingdienst mogelijk maakt.

“Personeel”, zoals door onderaannemers beheerd personeel: personen die de levering, administratie, beveiliging, beschikbaarheid of werking van de gecontroleerde dienst ondersteunen.

3. Controlecriterium C: gegevenslokalisatie in de Unie

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt c), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) bewijsmateriaal waaruit blijkt dat klantgegevens uitsluitend in de Unie worden opgeslagen en verwerkt en dat derden of onderaannemers die niet aan de voorwaarden van deze bijlage voldoen, onder geen beding technisch of operationeel in staat zijn om zonder voorafgaande toestemming klantgegevens in te zien, te verkrijgen, niet-beschikbaar te maken, te vernietigen of meer in het algemeen te verwerken. Voorbeelden hiervan zijn toegangslogs, beleid inzake toegang door ondersteuningspersoneel, registraties van bevoorrechte toegang, beleid inzake de bewaartermijn van back-ups, een diagram van de gegevensstromen waarin wordt aangegeven waar de gegevens van de klant worden opgeslagen, verwerkt en gerepliceerd en waar de back-ups zich bevinden. Bij de verwerking van persoonsgegevens, contracten met onderaannemers waaruit blijkt dat Verordening (EU) 2016/679 wordt nageleefd;
- (2) bewijs van log- en monitoringbestanden waaruit blijkt dat alle gegevens uitsluitend in de Unie worden opgeslagen en verwerkt. Voorbeelden hiervan zijn raamovereenkomsten inzake diensten, overeenkomsten inzake gegevensverwerking, contractuele overeenkomsten inzake de locatie waar gegevens worden opgeslagen of verwerkt, of een EU-gegevensgrens;
- (3) bewijsmateriaal (bv. contractuele overeenkomsten, logbestanden en procedures die aan openbare lichamen worden aangeboden) waaruit blijkt dat de gecontroleerde aanbieder en de onderaannemers die betrokken zijn bij de verlening van de

gecontroleerde dienst de nodige maatregelen hebben getroffen om ervoor te zorgen dat:

- (a) klantgegevens, inclusief versleutelde gegevens, niet buiten de Unie worden doorgegeven zonder toestemming van het openbaar lichaam;
 - (b) gegevens niet worden doorgegeven aan andere derden dan onderaannemers die betrokken zijn bij de verlening van de dienst of ontvangers die daar uitdrukkelijk toestemming voor hebben gekregen van het openbaar lichaam;
- (4) een gegevensstroomdiagram met de gegevensstromen tussen de aanbieder van cloudcomputingdiensten en klantgegevens, alsook met betrekking tot diensten van derden en onderaannemers. In het diagram moeten de bron en de bestemming van de gegevens duidelijk worden aangegeven en moet worden aangetoond dat de gegevens de Unie niet verlaten.

NB: Voor de toepassing van deze bijlage wordt onder “klant” verstaan een openbaar lichaam dat een contractuele of andere juridisch bindende regeling is aangegaan met de aanbieder van cloudcomputingdiensten met het oog op de toegang tot of het gebruik van de cloudcomputingdienst.

“Klantgegevens”: gegevens waarover de klant van de cloudcomputingdiensten zeggenschap heeft, op wettelijke, contractuele of andere wijze, die:

- (a) *input zijn voor de cloudcomputingdienst door of namens de klant, inclusief authenticatiegegevens;*
- (b) *worden geproduceerd als gevolg van het gebruik van de cloudcomputingdienst door de klant.*

Klantgegevens kunnen ook gegevens omvatten waar de gecontroleerde aanbieder zeggenschap over heeft en die worden afgeleid als gevolg van de interactie met de gecontroleerde dienst door de klant van de clouddienst. Dit omvat klantgegevens en alle gegevens die voortvloeien uit het gebruik van cloudcomputingdiensten (d.w.z. telemetrie, metagegevens).

“Van cloudcomputingsdiensten afgeleide gegevens” omvatten het deel van logbestanden met gegevens over wie de dienst heeft gebruikt en op welk tijdstip, welke functies zijn gebruikt, welke soorten gegevens hierbij waren betrokken enz. Het kan ook gaan om informatie over het aantal gemachtigde gebruikers en hun identiteit. Het kan ook gaan om configuratie- of personaliseringsgegevens, wanneer de cloudcomputingdienst dergelijke configuratie- en personaliseringsfuncties heeft.

4. Controlecriterium D: burgerschap van de Unie

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt d), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) de gecontroleerde aanbieder moet de controleorganisatie bewijs leveren dat maatregelen zijn genomen om ervoor te zorgen dat, indien een openbaar lichaam verzoekt om burgerschap van de Unie, het personeel dat betrokken is bij de verlening van de gecontroleerde dienst burgers van de Unie zijn. Dit kan worden aangetoond aan de hand van geldige officiële door de overheid afgegeven documenten (bv. een geldig paspoort en een geldige nationale identiteitskaart);
- (2) de gecontroleerde aanbieder moet organisatieschema's en functieomschrijvingen verstrekken waarmee wordt bevestigd dat er op verzoek voor kan worden gezorgd

dat alleen personeel met het burgerschap van de Unie toegang heeft tot de werking, het beheer, het onderhoud en de ondersteuning van de gecontroleerde dienst;

- (3) de gecontroleerde aanbieder moet documenten verstrekken waaruit het beleid inzake toegangscontrole blijkt en controlesporen waaruit blijkt dat alleen bevoegd personeel met het burgerschap van de Unie toegang heeft tot de systemen en gegevens van de dienst;
- (4) de gecontroleerde aanbieder moet aantonen dat er procedures zijn waarin wordt beschreven hoe vóór de aanstelling het burgerschap wordt geverifieerd en hoe de naleving van dit controlecriterium gedurende het gehele dienstverband wordt gehandhaafd.

NB: Het personeel dat betrokken is bij de verlening van de gecontroleerde dienst kan bestaan uit personeel dat logische of fysieke toegang heeft tot de infrastructuur en de activa die worden gebruikt voor de cloudcomputingdienst, alsook personeel dat verantwoordelijk is voor klantenondersteuning, en al het personeel dat op managementniveau zeggenschap heeft over de aanbieder van cloudcomputingdiensten.

5. Controlecriterium E: op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregeling

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt e), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) een geldig Europees cyberbeveiligingscertificaat dat is afgegeven door een bevoegde conformiteitsbeoordelingsinstantie en waaruit blijkt dat de gecontroleerde dienst is beoordeeld en in overeenstemming is bevonden met de eisen voor de zekerheidsniveaus “basis”, “substantieel” of “hoog” in het kader van een Europese cyberbeveiligingscertificeringsregeling die is vastgesteld op grond van Verordening (EU) 2019/881, op voorwaarde dat een dergelijke regeling is vastgesteld;
- (2) een certificeringsverslag met een beschrijving van de belangrijkste componenten die zijn gebruikt voor de ontwikkeling en werking van de cloudcomputingdienst waarop het controlecertificaat betrekking heeft;
- (3) totdat de Europese cyberbeveiligingscertificeringsregeling voor cloudcomputingdiensten is vastgesteld, kan de gecontroleerde aanbieder de naleving aantonen door middel van geldige cyberbeveiligingscertificaten. Daaronder vallen onder meer, maar niet uitsluitend:
 - (a) een geldig certificaat dat is afgegeven door een bevoegde conformiteitsbeoordelingsinstantie (overeenkomstig CEN/CLC/TS 18072:2025), waaruit blijkt dat de cloudcomputingdienst is beoordeeld en in overeenstemming is bevonden met de eisen die overeenkomen met de in CEN/TS 18026:2024 vastgestelde zekerheidsniveaus “basis”, “substantieel” of “hoog”;
 - (b) een geldig certificaat dat is afgegeven door de relevante nationale bevoegde autoriteit waaruit blijkt dat de cloudcomputingdienst is beoordeeld en in overeenstemming is bevonden met de eisen van de nationale cyberbeveiligingsregeling die momenteel in de lidstaat van kracht is;
 - (c) bij gebrek aan een nationale regeling, bewijsmateriaal waaruit blijkt dat wordt voldaan aan het hoogste niveau van de op de markt beschikbare cyberbeveiligingsnormen.

6. Controlecriterium F: AI-systemen die worden geëxploiteerd door een derde land of een juridische entiteit in een derde land

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt f), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) contractbepalingen waarin wordt bepaald dat gegevens die worden verwerkt of gegenereerd door het gebruik van de gecontroleerde dienst, inclusief klantgerelateerde gegevens, logbestanden en telemetriegegevens, niet zullen worden gebruikt om AI-modellen of -systemen die door een derde land of een juridische entiteit in een derde land worden geëxploiteerd, te trainen of te verfijnen, en in geen geval buiten de Unie worden doorgegeven;
- (2) contractbepalingen waarin wordt gespecificeerd dat gegevens uitsluitend worden verwerkt voor de levering van de gecontroleerde dienst en niet voor verbeteringen van de dienst of model- of systeemverbeteringen of andere secundaire doeleinden;
- (3) gegevensstroomdiagrammen die de end-to-end gegevensstroom documenteren, waaronder het invoeren, opslaan, verwerken en wissen van gegevens. De diagrammen moeten ook laten zien waar de AI-pijplijnen of activiteiten op het gebied van machinaal leren (MLOps) in verbinding staan met de klantgegevens;
- (4) MLOps of gebruiksgegevens waaruit blijkt dat de bouw-, test- en bekendmakingslocaties zich in de EU bevinden;
- (5) model- of systeemkaarten met daarop de naam van het model of systeem, de versie, de trainings- en valideringsbronnen, inclusief verklaringen dat de door het gebruik van de gecontroleerde dienst gegenereerde gegevens de Unie niet verlaten;
- (6) beleid inzake de herkomst van gegevens en bijbehorende uitvoeringsdocumentatie waaruit blijkt dat de aanbieder instrumenten voor de herkomst en bronnen van de gegevens gebruikt en die (per gegevensbestand) kunnen aantonen waarvoor de gegevens zijn gebruikt;
- (7) een lijst van de onderaannemers (met vermelding van hun land van vestiging) die toegang hebben tot de gegevens die door het gebruik van de gecontroleerde dienst zijn gegenereerd.

7. Controlecriterium G: geen zeggenschap van een derde land of geen zeggenschap van een entiteit in een derde land

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt g), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) de controleorganisatie moet het volgende vaststellen en analyseren:
 - (a) alle directe en indirecte aandeelhouders, tot aan de uiteindelijke eigenaars;
 - (b) de kapitalisatietabel die de eigendomsstructuur van de onderneming documenteert;
 - (c) het orgaan of de organen die bevoegd zijn om strategische besluiten te nemen (algemene vergadering van aandeelhouders, raad van toezicht, raad van bestuur enz.);
 - (d) de regels voor benoeming/verkiezing/ontslag van bestuursorganen en de feitelijke samenstelling van de bestuursorganen (bv. om na te gaan of een aandeelhouder het recht heeft een bestuurder te benoemen of de meerderheid van het aantal zetels in de raad van bestuur heeft);

- (e) de quorums en meerderheden die vereist zijn voor de vaststelling van strategische besluiten, om te bepalen of een aandeelhouder een strategisch besluit kan nemen (hetzij omdat hij de vereiste meerderheid heeft om een dergelijk besluit goed te keuren, hetzij omdat hij een dergelijk besluit kan blokkeren door middel van een veto of andere specifieke rechten, zelfs als hij een dergelijk besluit niet zelf kan opleggen enz.);
 - (f) de mogelijke invloed op strategische besluiten via commerciële betrekkingen, financiële betrekkingen of andere middelen enz.
- (2) De gecontroleerde aanbieder moet al deze informatie opvragen bij zijn onderaannemers en ter beschikking stellen van de controleorganisatie.

7.1. Beoordeling van eigendom en zeggenschap

- (1) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot het hoofdkantoor:
- (a) de plaats en het volledige adres van het algemene hoofdkantoor en/of de hoofdvestiging;
 - (b) de locaties van de uitvoerende bestuursstructuren.
- (2) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot de eigendomsstructuur en specifieke rechten:
- (a) een gedetailleerde lijst van eigenaren die:
 - i. direct of indirect ten minste 5 % van het kapitaal of ten minste 5 % van de stemrechten bezitten, onder meer via inhoud, afspraak, betrekking of tussenpersoon. Dit omvat stemafspraken tussen aandeelhouders die samen meer dan 5 % van de stemrechten of 5 % van het kapitaal zouden hebben;
 - ii. een of meer van de volgende specifieke rechten hebben met betrekking tot hun eigendom: a) het recht om een veto uit te spreken tegen een overdracht van aandelen; b) voorkeursrechten; c) het recht om onder voorwaarden extra aandelen te kopen of te beleggen;
 - (b) de controleorganisatie dient de volgende bewijsstukken op te vragen om de elementen in lid 2, punt a), te beoordelen:
 - i. uittreksels uit het handelsregister en het register van aandeelhouders van de organisatie en alle andere relevante documenten waarin de aandeelhouders en hun stemrechten of het percentage van hun belang duidelijk worden vermeld;
 - ii. aandeelhoudersovereenkomsten, memoranda van overeenstemming tussen aandeelhouders, statuten of andere relevante documenten met betrekking tot de besluitvormingsprocedures binnen de juridische entiteit, investeringsovereenkomsten tussen de aandeelhouders enz.;
 - iii. voor aandeelhouders die rechtspersonen zijn die ten minste 5 % van het kapitaal of ten minste 5 % van de stemrechten bezitten:
 - (1) een diagram met een beschrijving van de verschillende eigendomslagen/de zeggenschapsketen tot aan de uiteindelijke eigenaars;
 - (2) de statuten of gelijkwaardige oprichtingsakten;

- (3) een register van directeuren, functionarissen en tekenbevoegde personen.
- (3) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot de corporate governance:
- (a) de gecontroleerde aanbieder verstrekt de controleorganisatie een beschrijving van:
- i. de besluitvormingsorganen, de samenstelling ervan en de nationaliteit of plaats van vestiging van de leden ervan (indien van toepassing);
 - ii. de regels voor de verkiezing, aanstelling, benoeming of termijn van leden van de besluitvormingsorganen of andere personen in leidinggevende functies;
 - iii. de besluitvormingsprocedures, inclusief informatie over de vereiste meerderheid en/of het vereiste quorum voor besluiten;
 - iv. intern governancebeleid waarin wordt beschreven hoe eigendoms- en zeggenschapsbesluiten worden vastgelegd en goedgekeurd;
- besluiten van de raad van bestuur en het management die de vermelde zeggenschapsstructuur weerspiegelen;
- notulen van vergaderingen van de raad van bestuur en bestuursbesluiten inzake wijzigingen in de zeggenschap;
- (b) de gecontroleerde aanbieder moet de controleorganisatie bewijsstukken verstrekken waarin het volgende wordt uiteengezet of beschreven: de besluitvormingsorganen en de regels inzake hun verkiezing, aanstelling, benoeming of termijn, besluitvormingsprocedures, stemrechten, vetorechten, benoemingsrechten, goedkeuringsrechten binnen de juridische entiteit (bv. statuten, verslagen over corporate governance enz.). De ondersteunende documenten en informatie moeten worden verstrekt voor elke intermediaire juridische entiteit die direct of indirect 5 % of meer van het kapitaal of de stemrechten bezit, tot aan de uiteindelijke eigenaars van alle betrokken lagen.
- (4) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot het zeggenschap:
- (a) de gecontroleerde aanbieder verstrekt de controleorganisatie bewijs van de commerciële betrekkingen die zeggenschap verlenen. Dit omvat, maar is niet beperkt tot, een lijst van personen of juridische entiteiten waarmee de gecontroleerde aanbieders (of de eigenaren van de gecontroleerde aanbieder, inclusief tussenlagen tot aan de uiteindelijke eigenaren) een commerciële betrekking hebben die a) leidt tot een vergelijkbaar niveau van zeggenschap over het beheer en de middelen als de eigendom van aandelen of activa; en b) van zeer lange duur is (bv. zeer belangrijke langlopende leveringsovereenkomsten of kredieten die door softwarefabrikanten/klanten worden verstrekt, in combinatie met structurele betrekkingen);
- (b) de ondersteunende documenten moeten samenwerkingsovereenkomsten met het openbaar lichaam of softwarefabrikanten enz. omvatten.
- (5) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot de financiële betrekkingen die zeggenschap verlenen:

- (a) de gecontroleerde aanbieder moet een lijst opstellen van de personen of juridische entiteiten (inclusief aandeelhouders of eigenaren met zeggenschap) waarvan de gecontroleerde aanbieder (of de eigenaren) financieel afhankelijk is (zijn), op een wijze die hen in staat zou kunnen stellen concessies te verkrijgen op strategische bedrijfsgebieden;
 - (b) de ondersteunende documenten moeten leningdocumenten, statuten en documenten waaruit de financiële betrekking blijkt, enz. omvatten.
- (6) De gecontroleerde aanbieder verstrekt de controleorganisatie de volgende bewijsstukken met betrekking tot andere zeggenschapsbronnen:
- (a) de gecontroleerde aanbieder moet de controleorganisatie meedelen of er andere middelen, processen of betrekkingen zijn die uiteindelijk zeggenschap verlenen aan een ander derde land of een in een derde land gevestigde juridische entiteit (vergelijkbaar niveau van zeggenschap over het beheer en de middelen als de eigendom van aandelen of activa en van lange duur);
 - (b) de bewijsstukken moeten het bewijs leveren van een dergelijke zeggenschap of een verklaring dat er geen sprake is van een dergelijke zeggenschap (deze verklaring kan afkomstig zijn van de raad van bestuur van de dienstverlener).

NB: De elementen waarmee rekening moet worden gehouden bij de beoordeling van zeggenschap zijn de eigendomsstructuren en specifieke rechten, corporate governance, commerciële betrekkingen die zeggenschap verlenen, financiële betrekkingen die zeggenschap verlenen en alle andere bronnen van zeggenschap.

7.2. Aanvullende stappen op basis van de conclusie van de eigendoms- en zeggenschapstoets

Indien de controleorganisatie vaststelt dat de gecontroleerde aanbieder onder zeggenschap staat van een derde land of een juridische entiteit in een derde land, moet zij om het volgende aanvullende bewijs verzoeken:

- (c) bewijsstukken waaruit blijkt dat de Commissie op grond van artikel 19 een besluit heeft vastgesteld met betrekking tot het derde land dat zeggenschap uitoefent over de aanbieder van cloudcomputingdiensten;
- (d) alle bewijsstukken waaruit blijkt dat de gecontroleerde aanbieder en eventuele onderaannemers die bij de verlening van de gecontroleerde dienst betrokken zijn, de nodige maatregelen hebben getroffen om de doeltreffende juridische, technische en organisatorische scheiding tussen de aanbieder van cloudcomputingdiensten en een derde land of een in een derde land gevestigde juridische entiteit te handhaven, om ervoor te zorgen dat de aanbieder van cloudcomputingdiensten juridisch, technisch en operationeel niet in staat is te voldoen aan verzoeken om toegang tot klantgegevens, inclusief versleutelde gegevens, of om de continuïteit van de dienst te verstoren of de kwaliteit van de dienst aan te tasten;
- (e) alle bewijsstukken waaruit blijkt dat het openbaar lichaam in kennis zal worden gesteld van een dergelijk verzoek en een bevestiging dat het verzoek is afgewezen;
- (f) alle bewijsstukken waaruit blijkt dat een register wordt bijgehouden van alle verzoeken om toegang tot klantgegevens, om de continuïteit van de dienstverlening te verstoren of om de kwaliteit van de dienstverlening aan te

tasten van een derde land of een in een derde land gevestigde juridische entiteit, dat ten minste het verzoek en het antwoord op het verzoek bevat.

8. Controlecriterium H: geen technische en operationele ondersteuning buiten de Unie

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt h), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) bewijs dat de gecontroleerde aanbieder bindende contractbepalingen uitvoert waarin staat dat alle ondersteunende, administratieve, onderhouds-, monitoring-, incidentrespons- en operationele activiteiten uitsluitend in de Unie mogen worden geïnitieerd en uitgevoerd. Dit kunnen contractbepalingen zijn die voorafgaande bekendmaking van alle onderaannemers en ondersteunende locaties vereisen, voorafgaande schriftelijke toestemming alvorens nieuwe onderaannemers in dienst worden genomen, en een recht om onderaannemers die buiten de Unie zijn gevestigd, te weigeren;
- (2) bewijs dat de gecontroleerde aanbieder een actueel register van onderaannemers bijhoudt;
- (3) bewijs dat de gecontroleerde aanbieder dergelijke activiteiten niet uitbesteedt of overdraagt buiten de Unie;
- (4) bewijs dat de gecontroleerde aanbieder de nodige wettelijke, technische en organisatorische maatregelen heeft getroffen om ervoor te zorgen dat er geen toegang op afstand kan zijn voor technische en operationele ondersteuning van buiten de Unie voor de gecontroleerde dienst;
- (5) bewijs dat de helpdesk-/ondersteuningsdiensten van de gecontroleerde aanbieder, het beheer van de infrastructuur, de activiteiten van het operationeel beveiligingscentrum of netwerkexploitatiecentrum, bevoorrechte toegang, verwerking van back-ups en herstelactiviteiten na calamiteiten van de gecontroleerde dienst uitsluitend vanuit de Unie worden verleend, inclusief het toegangstraject voor het beheer van de dienst;
- (6) bewijs dat de gecontroleerde aanbieder ervoor zorgt dat het personeel na het verlaten van de onderneming geen toegang meer heeft tot de gecontroleerde dienst en dat alle toegangsrechten worden ingetrokken;
- (7) bewijs dat de gecontroleerde aanbieder de nodige technische en organisatorische maatregelen heeft getroffen om ervoor te zorgen dat de administratieve toegang tot systemen die worden gebruikt om de gecontroleerde dienst te exploiteren, wordt verleend via toegangstrajecten binnen de Unie. Dit kan worden aangetoond door de uitvoering van geografisch beperkte netwerkbesturing, administratieve infrastructuur in de Unie, controles op het beheer van bevoorrechte toegang en monitoringmechanismen;
- (8) bewijs dat de gecontroleerde aanbieder over procedures beschikt waaruit blijkt dat er geen effectieve zeggenschap is van een derde land of een in een derde land gevestigde juridische entiteit, ook bij latere onderaanbesteding.

9. Controlecriterium I: waarborgen van de transparantie van de toeleveringsketen van software

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt i), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) de gecontroleerde aanbieder verstrekt de controleorganisatie een volledige en actuele softwarestuklijst voor alle softwarecomponenten, waaronder opensourcesoftware (OSS);
- (2) de gecontroleerde aanbieder verstrekt de controleorganisatie een lijst van afhankelijkheden. Hierbij gaat het om:
 - (a) alle gebruikte softwaremodules, bibliotheken of applicatieprogramma-interfaces (API's), alsmede ontwikkelingsinstrumenten;
 - (b) oorsprong van de software: waar (land van oorsprong) en door wie de software is ontworpen, is ontwikkeld en wordt onderhouden, de locatie van en rechtsgebied dat van toepassing is op de distributie van de software, en updates;
 - (c) de mate van afhankelijkheid van leveranciers, faciliteiten of eigendoms technologieën van buiten de EU; voor niveau 3, bewijs dat er, indien de softwarestack wordt geleverd door een juridische entiteiten in een derde land, geen onnodig ongerechtvaardigde licentiebeperkingen gelden;
 - (d) de mate van afhankelijkheid van opensourcesoftware;
 - (e) de zichtbaarheid van de volledige keten van softwarefabrikanten en subfabrikanten, waaronder auditrechten;

NB: De bovenstaande vereisten impliceren dat joint ventures, bijvoorbeeld van een entiteit van de Unie met een in een derde land gevestigde juridische entiteit, voor dit niveau in aanmerking kunnen komen.

- (3) de gecontroleerde aanbieder verstrekt het volgende:
 - (a) bewijs van een risicogebaseerd proces voor het identificeren en beperken van afhankelijkheden van externe softwarefabrikanten die relevant zijn voor de werking van de cloudcomputingdienst;
 - (b) bewijs dat er één of meer alternatieve softwareoplossingen, waaronder opensourcesoftware, zijn geïdentificeerd. Indien geen gelijkwaardige software kan worden geïdentificeerd, moet een oplossing worden gevonden die een minimaal werkbare functionaliteit waarborgt. Er moeten tests worden uitgevoerd en er moet een overschakelingsplan worden opgesteld om de migratie naar dergelijke alternatieve oplossingen mogelijk te maken;
 - (c) bewijs dat kan worden overgeschakeld naar een alternatieve oplossing in geval van een defect of verzuim van de verkoper of beperkingen van een derde land of een in een derde land gevestigde juridische entiteit;
 - (d) een lijst van open normen die worden gevolgd als onderdeel van het beleid van de gecontroleerde aanbieder met betrekking tot de gecontroleerde dienst;
- (4) de gecontroleerde aanbieder moet transparantie waarborgen door middel van toegang op afstand en controleerbaarheid van de broncode door:
 - (a) een lijst van bewijsstukken aan de controleorganisatie te verstrekken om aan te tonen dat er geen gebruik wordt gemaakt van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren. Hierbij gaat het om:
 - i. bewijs in verband met het testen van de softwarecomponent om het gebruik te voorkomen van functies of mechanismen op afstand die

- kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren (testprocedure, testverslagen, testplan enz.);
 - ii. bewijs dat de procedures van de organisatie op het gebied van wijzigingsbeheer alle wijzigingen in firmware, bios en software-updates omvatten, alsook de integratie van nieuwe componenten, om het gebruik van functies of mechanismen op afstand te voorkomen;
 - iii. bewijs dat de onderhoudsprocedure is geactualiseerd om onder meer te voorkomen dat een functie of mechanisme op afstand wordt gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren;
- (b) de gecontroleerde aanbieder moet ervoor zorgen dat de onafhankelijke externe controleur toegangsrechten krijgt voor de broncode van dergelijke software en deze kan controleren. De gecontroleerde aanbieder moet er ook voor zorgen dat alle documentatie, technische documenten en informatie die nodig is om de broncode te evalueren en te controleren, in een volledig, nauwkeurig en toegankelijk formaat ter beschikking van de controleorganisatie worden gesteld.

10. Controlecriterium J: opensourcesoftware

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt j), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) de gecontroleerde aanbieder moet transparantie waarborgen door middel van toegang op afstand en controleerbaarheid van de broncode door:
 - (a) een lijst van bewijsstukken aan de controleorganisatie te verstrekken om aan te tonen dat er geen gebruik wordt gemaakt van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren. Hierbij gaat het om:
 - i. bewijs in verband met het testen van de softwarecomponent om het gebruik te voorkomen van functies of mechanismen op afstand die kunnen worden gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren (testprocedure, testverslagen, testplan enz.);
 - ii. bewijs dat de procedures van de organisatie op het gebied van wijzigingsbeheer alle wijzigingen in firmware, bios en software-updates omvatten, alsook de integratie van nieuwe componenten, om het gebruik van functies of mechanismen op afstand te voorkomen;
 - iii. bewijs dat de onderhoudsprocedure is geactualiseerd om onder meer te voorkomen dat een functie of mechanisme op afstand wordt gebruikt om een apparaat, systeem of software wezenlijk te manipuleren of te verstoren;
- (2) de gecontroleerde aanbieder verstrekt het volgende:
 - (a) bewijs van een risicogebaseerd proces om het volgende vast te stellen en te beperken: i) een zwak ecosysteem en onvoldoende steun van de OSS-gemeenschap; ii) het ontbreken van continue monitoring van nieuw verschenen

updates; iii) gevallen waarin de opensourcesoftware verouderd is of niet langer wordt bijgehouden;

- (b) bewijs dat de gecontroleerde aanbieder de bijgewerkte OSS zonder onnodige vertraging heeft toegepast;
 - (c) bewijs dat de gecontroleerde aanbieder een of meer alternatieve opensourceoplossingen heeft vastgesteld. Indien de gecontroleerde aanbieder geen gelijkwaardige software kan identificeren, moet een oplossing worden gevonden die een minimale werkbare functionaliteit waarborgt. De gecontroleerde aanbieder moet tests uitvoeren en een overschakelingsplan opstellen om de migratie naar alternatieve oplossingen mogelijk te maken;
- (3) wanneer de gecontroleerde aanbieder software gebruikt die op grond van een opensourcelicentie is vrijgegeven, moet de gecontroleerde aanbieder mechanismen invoeren om het openbaar lichaam tijdig in kennis te stellen indien wordt ontdekt dat de software is verworven door of onder zeggenschap staat van een derde land of een in een derde land gevestigde juridische entiteit of stichting.

11. Controlecriterium K: mondiale diensten en dochterondernemingen in derde landen

De controleorganisatie moet het onder de Uniebetrouwbaarheidsniveaus 2, 3 en 4, punt k), van bijlage II vermelde controlecriterium beoordelen op basis van de volgende bewijsstukken:

- (1) de controleorganisatie moet nagaan of de dochteronderneming juridisch en operationeel onafhankelijk is van de gecontroleerde aanbieder;
- (2) de gecontroleerde aanbieder moet aantonen dat de dochteronderneming geen toegang heeft tot systemen voor de verwerking of opslag van klantgegevens;
- (3) de gecontroleerde aanbieder moet aantonen dat de dochteronderneming geen bevoorrechte accounts heeft binnen de productieomgevingen in de Unie, inclusief cloudbeheer, identiteits- en toegangsbeheer (IAM), beheer van bevoorrechte toegang (PAM), monitoring of databankbeheer;
- (4) de controleorganisatie moet nagaan of het personeel van de dochteronderneming geen toegang kan krijgen tot klantgegevens in de Unie;
- (5) de controleorganisatie moet nagaan of de dochteronderneming niet bevoegd is om operationeel personeel in de Unie op te dragen klantgegevens openbaar te maken of beveiligingsprocedures te omzeilen;
- (6) de controleorganisatie moet nagaan of alle door de dochteronderneming ontvangen verzoeken van buitenlandse regeringen formeel worden doorverwezen naar de bevoegde entiteit van de Unie voor juridische beoordeling op grond van het Unierecht en het lidstatelijke recht.