

I

(Wetgevingshandelingen)

VERORDENINGEN

VERORDENING (EU) 2021/887 VAN HET EUROPEES PARLEMENT EN DE RAAD**van 20 mei 2021****tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra**

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 173, lid 3, en artikel 188, eerste alinea,

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 Comité ⁽¹⁾,

Handelend volgens de gewone wetgevingsprocedure ⁽²⁾,

Overwegende hetgeen volgt:

- (1) De meerderheid van de bevolking van de Unie is verbonden met het internet. In het dagelijkse leven van mensen en in onze economieën steunen we steeds meer op digitale technologieën. Burgers en bedrijven worden steeds meer blootgesteld aan ernstige cyberbeveiligingsincidenten en vele bedrijven in de Unie krijgen ieder jaar te maken met ten minste één cyberbeveiligingsincident. Dit onderstreept dat weerbaarheid, grotere technologische en industriële vermogens, hoge cyberbeveiligingsnormen en holistische cyberbeveiligingsoplossingen nodig zijn waarbij mensen, producten, processen en technologie in de Unie betrokken zijn, alsook dat leiderschap van de Unie op het gebied van cyberbeveiliging en digitale autonomie nodig is. Cyberbeveiliging kan ook worden verbeterd door het bewustzijn over cyberdreigingen te verhogen en door in de hele Unie competenties, capaciteiten en vermogens te ontwikkelen, waarbij terdege rekening wordt gehouden met de maatschappelijke en ethische implicaties en bezwaren.
- (2) De Unie heeft haar activiteiten met betrekking tot de toenemende uitdagingen op het gebied van cyberbeveiliging stelselmatig uitgebreid in aansluiting op de strategie inzake cyberbeveiliging, die de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (hoge vertegenwoordiger) hebben gepresenteerd in hun gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 7 februari 2013, getiteld "Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace" (de "cyberbeveiligingsstrategie van 2013"). De cyberbeveiligingsstrategie van 2013 heeft tot doel een betrouwbaar, veilig en open cyber-ecosysteem tot stand te brengen. In 2016 heeft de Unie de eerste maatregelen op het gebied van cyberbeveiliging vastgelegd in Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ⁽³⁾ betreffende de beveiliging van netwerk- en informatiesystemen.

⁽¹⁾ PB C 159 van 10.5.2019, blz. 63.

⁽²⁾ Standpunt van het Europees Parlement van 17 april 2019 (nog niet bekendgemaakt in het Publicatieblad) en standpunt van de Raad in eerste lezing van 20 april 2021 (nog niet bekendgemaakt in het Publicatieblad). Standpunt van het Europees Parlement van 19 mei 2021 (nog niet bekendgemaakt in het Publicatieblad).

⁽³⁾ Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

- (3) De Commissie en de hoge vertegenwoordiger hebben in september 2017 aan het Europees Parlement en de Raad een gezamenlijke mededeling voorgesteld, getiteld “Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU” om de weerbaarheid, het afschrikkingseffect en het reactievermogen van de Unie ten opzichte van cyberaanvallen verder te versterken.
- (4) De staats- en regeringsleiders hebben op de digitale top van Tallinn in september 2017 opgeroepen om van Europa uiterlijk in 2025 een mondiale leider in cyberbeveiliging te maken, zodat de burgers, consumenten en bedrijven vol vertrouwen online kunnen gaan en bescherming genieten, en zodat een vrij, veiliger en aan het recht onderworpen internet mogelijk wordt, en hebben verklaard dat zij voornemens zijn meer gebruik te maken van open-sourceoplossingen en open normen bij het (om)bouwen van informatie- en communicatietechnologiesystemen en -oplossingen (ICT), met name om afhankelijkheid van één leverancier (vendor lock-in) te voorkomen, met inbegrip van die welke zijn ontwikkeld of bevorderd door programma's van de Unie voor interoperabiliteit en normalisatie, zoals ISA².
- (5) Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (het “kenniscentrum”) dat bij deze verordening wordt opgericht, moet de beveiliging van netwerk- en informatiesystemen, met inbegrip van het internet en andere infrastructuur die essentieel is voor de werking van de maatschappij, zoals vervoer, gezondheidszorg, energie, digitale infrastructuur, water, de financiële markten en de banksystemen, helpen vergroten.
- (6) Ernstige verstoringen van netwerk- en informatiesystemen kunnen gevolgen hebben voor individuele lidstaten en voor de Unie als geheel. Een hoge mate van beveiliging van netwerk- en informatiesystemen in de hele Unie is daarom essentieel zowel voor de maatschappij als voor de economie. Voor cyberbeveiliging is de Unie momenteel afhankelijk van niet-Europese aanbieders. Het is echter in het strategische belang van de Unie om essentiële onderzoeks- en technologische capaciteiten op het gebied van cyberbeveiliging te behouden en te ontwikkelen voor de beveiliging van netwerk- en informatiesystemen van burgers en bedrijven, met name de bescherming van vitale netwerk- en informatiesystemen en de verlening van essentiële diensten op het gebied van cyberbeveiliging.
- (7) In de Unie is er een overvloed aan deskundigheid en ervaring als het gaat om onderzoek, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging, maar de inspanningen van de industrie- en onderzoeksgemeenschappen zijn versnipperd, onvoldoende op elkaar afgestemd en niet gericht op een gezamenlijke missie, hetgeen het concurrentievermogen schaadt en de effectieve bescherming van netwerken en systemen op dat gebied hindert. Dergelijke inspanningen en deskundigheid moeten op een efficiënte manier gebundeld, in een netwerk ondergebracht en gebruikt worden om bestaande capaciteiten op het gebied van onderzoek, technologie en industriële capaciteiten en vaardigheden op Unieniveau en nationaal niveau te vergroten en aan te vullen. Hoewel de ICT-sector voor belangrijke uitdagingen staat, zoals voorzien in zijn behoefte aan bekwame arbeidskrachten, kan hij er baat bij hebben de diversiteit van de samenleving als geheel af te spiegelen, te zorgen voor evenwichtige gendervertegenwoordiging, etnische diversiteit en non-discriminatie van personen met een beperking, en de toegang te faciliteren tot kennis en opleiding voor toekomstige deskundigen op het gebied van cyberbeveiliging, met inbegrip van de opleiding van deze deskundigen in niet-formele contexten, bijvoorbeeld in projecten op het gebied van gratis en opensource-software, civic technology-projecten, start-ups en micro-ondernemingen.
- (8) Kleine en middelgrote ondernemingen (kmo's (mkb)) zijn cruciale stakeholders in de cyberbeveiligingssector van de Unie en kunnen dankzij hun beweeglijkheid de allernieuwste oplossingen bieden. Kmo's die niet in cyberbeveiliging gespecialiseerd zijn, zijn echter meestal kwetsbaarder voor cyberbeveiligingsincidenten, omdat voor het instellen van effectieve cyberbeveiligingsoplossingen grote investeringen en kennis nodig zijn. Daarom moeten het kenniscentrum en het netwerk van nationale coördinatiecentra (het “netwerk”) kmo's steun verlenen door de toegang van kmo's tot kennis te vergemakkelijken en door toegang op maat tot onderzoeks- en ontwikkelingsresultaten te bieden, zodat kmo's zichzelf voldoende kunnen beveiligen en zodat kmo's die actief zijn op het gebied van cyberbeveiliging kunnen concurreren en bijdragen tot de leidende positie van de Unie op het gebied van cyberbeveiliging.
- (9) Er bestaat expertise buiten de context van industrie en onderzoek. Niet-commerciële en precommerciële projecten, bekend onder de noemer van “civic technology”, maken gebruik van open normen, open data en gratis en opensource-software, ten dienste van de maatschappij en het algemeen belang.
- (10) Het gebied van cyberbeveiliging is divers. De betrokken stakeholders zijn afkomstig van openbare entiteiten, de lidstaten en de Unie, alsook van het bedrijfsleven, het maatschappelijk middenveld, zoals vakbonden, consumentenorganisaties, de gemeenschap voor vrije en opensource-software en de academische wereld en de onderzoeksgemeenschap, en andere entiteiten.
- (11) In de in november 2017 aangenomen conclusies van de Raad werd de Commissie verzocht een snelle effectbeoordeling te maken van de mogelijke opties om een netwerk van kenniscentra voor cyberbeveiliging en een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging op te richten en medio 2018 het relevante rechtsinstrument voor te stellen voor de creatie van een dergelijk netwerk en een dergelijk centrum.

- (12) Het ontbreekt de Unie nog steeds aan voldoende technologische en industriële capaciteiten en vermogens om haar economie en vitale infrastructuur zelfstandig te beveiligen en een wereldleider op het gebied van cyberbeveiliging te worden. Er is een gebrek aan strategische, duurzame coördinatie en samenwerking tussen bedrijfstakken, onderzoeksgemeenschappen op het gebied van cyberbeveiliging en overheden. De Unie ondervindt de nadelen van het feit dat er ontoereikende investeringen en beperkte toegang tot kennis, vaardigheden en faciliteiten op het gebied van cyberbeveiliging zijn, en slechts weinig resultaten van onderzoek en innovatie in de Unie op het gebied van cyberbeveiliging worden vertaald in commercieel interessante oplossingen of op grote schaal in de economie toegepast.
- (13) Het oprichten van het kenniscentrum en van het netwerk, met een mandaat om maatregelen te nemen ter ondersteuning van industriële technologieën en op het gebied van onderzoek en innovatie, is de beste manier om aan de doelstellingen van deze verordening te voldoen en tegelijkertijd optimale economische, maatschappelijke en ecologische effecten te bieden en de belangen van de Unie te beschermen.
- (14) Het kenniscentrum moet het belangrijkste instrument van de Unie zijn om investeringen in onderzoek, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging te bundelen en om samen met het netwerk relevante projecten en initiatieven uit te voeren. Het kenniscentrum moet financiële steun voor cyberbeveiliging beheren uit Horizon Europa, het kaderprogramma voor onderzoek en innovatie dat is vastgesteld bij Verordening (EU) 2021/695 van het Europees Parlement en de Raad⁽⁴⁾ (“Horizon Europa”), en uit het programma Digitaal Europa, dat is vastgesteld bij Verordening (EU) 2021/694 van het Europees Parlement en de Raad⁽⁵⁾ (het “programma Digitaal Europa”), en in voorkomend geval ook open staan voor andere programma’s. Deze aanpak moet bijdragen tot het creëren van synergieën en tot coördinatie van financiële steun voor initiatieven van de Unie op het gebied van onderzoek en ontwikkeling, innovatie, technologie en industriële ontwikkeling met betrekking tot cyberbeveiliging en moet vermijden dat er onnodig dubbel werk wordt verricht.
- (15) Het is van belang ervoor te zorgen dat de grondrechten en regels inzake ethisch gedrag worden geëerbiedigd bij onderzoeksprojecten op het gebied van cyberbeveiliging die door het kenniscentrum worden ondersteund.
- (16) Het kenniscentrum mag geen operationele taken op het gebied van cyberbeveiliging uitvoeren, zoals taken die verband houden met Computer Security Incident Response Teams (CSIRT’s), met inbegrip van het monitoren en aanpakken van cyberincidenten. Het kenniscentrum zou echter de ontwikkeling van ICT-infrastructuur ten dienste van het bedrijfsleven, met name kmo’s, onderzoeksgemeenschappen, het maatschappelijk middenveld en de overheidssector, kunnen faciliteren, in overeenstemming met de in deze verordening vastgelegde opdracht en doelstellingen. Wanneer CSIRT’s en andere stakeholders trachten de rapportage en openbaarmaking van kwetsbaarheden te bevorderen, moeten het kenniscentrum en de leden van de Kennisgemeenschap voor cyberbeveiliging (de “kennisgemeenschap”) deze stakeholders op hun verzoek kunnen ondersteunen binnen de grenzen van hun respectieve taken, en zonder overlapping met het Agentschap van de Europese Unie voor cyberbeveiliging (“Enisa”) zoals opgericht bij Verordening (EU) 2019/881 van het Europees Parlement en de Raad⁽⁶⁾.
- (17) Het is de bedoeling dat het kenniscentrum, de kennisgemeenschap en het netwerk voor het beheer van de kennisgemeenschap en de vertegenwoordiging van de kennisgemeenschap in het kenniscentrum profiteren van de ervaring en de brede vertegenwoordiging van relevante stakeholders, opgebouwd dankzij het contractuele publiek-private partnerschap voor cyberbeveiliging tussen de Commissie en de Europese organisatie voor cyberbeveiliging (ECISO) voor de looptijd van Horizon 2020 — het kaderprogramma voor onderzoek en innovatie (2014-2020), zoals vastgesteld bij Verordening (EU) nr. 1291/2013 van het Europees Parlement en de Raad⁽⁷⁾, van de lessen die zijn getrokken uit vier proefprojecten die begin 2019 in het kader van Horizon 2020 zijn gestart, namelijk Concordia, ECHO, Sparta en CyberSec4Europe, en van het proefproject en de voorbereidende actie inzake Free and Open Source Software Audits (EU Fossa).
- (18) Gezien de omvang van de uitdaging op het gebied van cyberbeveiliging en gezien de investeringen in cyberbeveiligingscapaciteiten en -vermogens in andere delen van de wereld, moeten de Unie en de lidstaten worden aangemoedigd hun financiële steun voor onderzoek, ontwikkeling en invoering op dit gebied te vergroten. Om schaalvoordelen te realiseren in een vergelijkbaar beschermingsniveau in de gehele Unie te bereiken, moeten de lidstaten hun inspanningen in een uniaal kader plaatsen door actief bij te dragen aan het werk van het kenniscentrum en het netwerk.

⁽⁴⁾ 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, en tot vaststelling van de regels voor deelname en verspreiding, en tot intrekking van de Verordeningen (EU) nr. 1290/2013 en (EU) nr. 1291/2013 (PB L 170 van 12.5.2021, blz. 1).

⁽⁵⁾ Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot vaststelling van het programma Digitaal Europa, en tot intrekking van Besluit (EU) 2015/2240 (PB L 166 van 11.5.2021, blz. 1).

⁽⁶⁾ Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

⁽⁷⁾ Verordening (EU) nr. 1291/2013 van het Europees Parlement en de Raad van 11 december 2013 tot vaststelling van Horizon 2020 — het kaderprogramma voor onderzoek en innovatie (2014-2020) en tot intrekking van Besluit nr. 1982/2006/EG (PB L 347 van 20.12.2013, blz. 104).

- (19) Ter bevordering van het concurrentievermogen van de Unie en hoge internationale cyberbeveiligingsnormen moeten het kenniscentrum en de kennisgemeenschap streven naar uitwisseling over de ontwikkelingen op het gebied van cyberbeveiliging, ook op het gebied van producten en processen, van normen en van technische normen, met de internationale gemeenschap, indien dit van belang is voor de opdracht, de doelstellingen en de taken van het kenniscentrum. Toepasselijke technische normen kunnen voor de doelstellingen van deze verordening onder meer zijn de creatie van referentie-implementaties, inclusief die welke worden gepubliceerd in het kader van open standaardlicenties.
- (20) De zetel van het kenniscentrum is in Boekarest.
- (21) Het kenniscentrum moet bij het opstellen van zijn jaarlijkse werkprogramma (jaarlijks werkprogramma) de Commissie in kennis stellen van zijn medefinancieringsbehoeften, zulks op basis van de geplande medefinancieringsbijdragen van de lidstaten aan gezamenlijke acties, zodat de Commissie bij het opstellen van het ontwerp van de algemene Uniebegroting voor het daaropvolgende jaar de overeenkomstige Uniebijdrage in aanmerking kan nemen.
- (22) De Commissie moet bij het opstellen van het deel van het werkprogramma van Horizon Europa dat verband houdt met cyberbeveiliging, ook bij de procedure voor raadpleging van stakeholders en in het bijzonder voorafgaand aan de vaststelling van dat werkprogramma, rekening houden met de input van het kenniscentrum en moet die input meedelen aan het programmacomit  van Horizon Europa.
- (23) Het kenniscentrum moet worden opgericht als een Unieorgaan met rechtspersoonlijkheid waarop Gedelegeerde Verordening (EU) 2019/715 van de Commissie⁽⁸⁾ van toepassing is, zodat het zijn rol op het gebied van cyberbeveiliging kan spelen, de betrokkenheid van het netwerk wordt gefaciliteerd, en teneinde ervoor te zorgen dat de lidstaten een sterke rol op het gebied van governance wordt toebedeeld. Het kenniscentrum moet een dubbele rol vervullen, namelijk specifieke taken uitvoeren met betrekking tot industrie, technologie en onderzoek op het gebied van cyberbeveiliging, zoals vastgelegd in deze verordening, en tegelijkertijd zorgen voor het beheer van cyberbeveiligingsgerelateerde financiering uit verschillende programma's, met name uit Horizon Europa en het programma Digitaal Europa, en mogelijk ook uit andere Unieprogramma's. Dat beheer zou moeten voldoen aan de voor die programma's geldende regels. Aangezien de werking van het kenniscentrum voornamelijk zal worden gefinancierd uit Horizon Europa en het programma Digitaal Europa, moet het kenniscentrum, wat betreft de uitvoering van de begroting, ook tijdens de programmeringsfase niettemin worden beschouwd als een partnerschap.
- (24) Als gevolg van de bijdrage van de Unie dient de toegang tot de resultaten van de activiteiten en projectresultaten van het kenniscentrum zo open mogelijk en zo gesloten als nodig te zijn, en dient hergebruik van deze resultaten in voorkomend geval mogelijk te zijn.
- (25) Het kenniscentrum moet de werkzaamheden van het netwerk bevorderen en co rdineren. Het netwerk moet bestaan uit   n nationaal co rdinatiecentrum per lidstaat. Nationale co rdinatiecentra waarvan de Commissie heeft erkend dat zij over de nodige capaciteit beschikken om middelen te beheren teneinde de in deze verordening vastgelegde opdracht en doelstellingen te verwezenlijken, moeten rechtstreekse Financi le steun van de Unie ontvangen, met inbegrip van subsidies die zonder oproep tot het indienen van voorstellen worden toegekend, om hun activiteiten in verband met deze verordening uit te voeren.
- (26) De nationale co rdinatiecentra moeten door de lidstaten geselecteerde publiekrechtelijke entiteiten of entiteiten met een overwegend publiekrechtelijk belang zijn, die openbarediensttaken verrichten krachtens het nationale recht, onder meer door middel van bevoegdheidsdelegatie. De taken van een nationaal co rdinatiecentrum in een lidstaat moeten kunnen worden uitgevoerd door een entiteit die ook andere taken krachtens het Unierecht verricht, zoals die van een nationaal bevoegde autoriteit, een centraal contactpunt in de zin van Richtlijn (EU) 2016/1148 of een andere verordening van de Unie, of een digitale-innovatiehub als bedoeld in Verordening (EU) 2021/694. Andere publiekrechtelijke entiteiten of entiteiten die in een lidstaat openbarediensttaken verrichten, moeten het nationale co rdinatiecentrum in die lidstaat bij de uitoefening van zijn taken kunnen bijstaan.
- (27) De nationale co rdinatiecentra moeten de noodzakelijke administratieve capaciteit bezitten, beschikken over, of toegang hebben tot, industri le, technologische en onderzoekdeskundigheid op het gebied van cyberbeveiliging en effectief in dialoog kunnen gaan en samenwerken met de industrie, de overheidssector en de onderzoeksgemeenschap.
- (28) In het onderwijs in de lidstaten moet het belang van voldoende bekendheid met en het hebben van vaardigheden op het gebied van cyberbeveiliging terug te zien zijn. Daartoe en rekening houdend met de rol van Enisa en onverminderd de bevoegdheden van de lidstaten op het gebied van onderwijs, moeten de nationale co rdinatiecentra, samen met de bevoegde overheidsinstanties en belanghebbenden, bijdragen aan de bevordering en verspreiding van onderwijsprogramma's op het gebied van cyberbeveiliging.

⁽⁸⁾ Gedelegeerde Verordening (EU) 2019/715 van de Commissie van 18 december 2018 houdende de Financi le kaderregeling van de bij het VWEU en het Euratom-Verdrag opgerichte organen, bedoeld in artikel 70 van Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad (PB L 122 van 10.5.2019, blz. 1).

- (29) De nationale coördinatiecentra moeten subsidies van het kenniscentrum kunnen ontvangen om financiële steun aan derden te verlenen in de vorm van subsidies. De directe kosten die door de nationale coördinatiecentra worden gemaakt voor de verlening en het beheer van financiële steun aan derden moeten in aanmerking komen voor financiering in het kader van de desbetreffende programma's.
- (30) Het kenniscentrum, het netwerk en de kennissamenleving moeten bijdragen tot de bevordering en verspreiding van de nieuwste cyberbeveiligingsproducten, -diensten en -procedures. Tegelijkertijd moeten het kenniscentrum en het netwerk de cyberbeveiligingsvermogens aan de vraagzijde van de industrie bevorderen, met name door ontwikkelaars en exploitanten te ondersteunen in sectoren zoals vervoer, energie, gezondheidszorg, financiën, overheid, telecommunicatie, maakindustrie en ruimtevaart, teneinde deze ontwikkelaars en exploitanten te helpen hun problemen op het gebied van cyberbeveiliging op te lossen, zoals door het toepassen van security by design. Het kenniscentrum en het netwerk moeten ook de standaardisering en de uitrol van cyberbeveiligingsproducten, -diensten en -procedures ondersteunen en, waar mogelijk, de implementatie bevorderen van het Europees kader voor cyberbeveiligingscertificering dat is vastgesteld bij Verordening (EU) 2019/881.
- (31) Omdat cyberdreigingen en cyberbeveiliging snel veranderen, moet de Unie zich snel en voortdurend kunnen aanpassen aan nieuwe ontwikkelingen op dit gebied. Het kenniscentrum, het netwerk en de kennissamenleving moeten daarom flexibel genoeg zijn om het vereiste reactievermogen inzake dergelijke ontwikkelingen te waarborgen. Zij moeten projecten vergemakkelijken die entiteiten in staat stellen continu vermogens op te bouwen om hun eigen weerbaarheid en die van de Unie te vergroten.
- (32) Het kenniscentrum moet de kennissamenleving ondersteunen. Het kenniscentrum moet de relevante met cyberbeveiliging verband houdende delen van Horizon Europa en het programma Digitaal Europa uitvoeren overeenkomstig het meerjarige werkprogramma van het kenniscentrum ("meerjarig werkprogramma"), het jaarlijkse werkprogramma en het strategisch planningsproces van Horizon Europa door subsidies en andere vormen van financiering toe te kennen, voornamelijk na uitschrijving van een oproep tot het indienen van voorstellen. Het kenniscentrum moet ook de overdracht van deskundigheid binnen zowel het netwerk als de kennissamenleving faciliteren en gezamenlijke investeringen door de Unie, de lidstaten of de industrie ondersteunen. Daarbij moet het bijzondere aandacht besteden aan het ondersteunen van kmo's op het gebied van cyberbeveiliging en aan acties die de vaardigheidskloof helpen dichten.
- (33) Technische bijstand voor de voorbereiding van projecten moet op volledig objectieve en transparante wijze worden verleend zodat alle potentiële begunstigden dezelfde informatie ontvangen en dient belangenconflicten te voorkomen.
- (34) Het kenniscentrum moet een stimulans geven en ondersteuning bieden voor langdurige strategische samenwerking en coördinatie van de activiteiten van de kennissamenleving, waarbij een grote, open, interdisciplinaire en diverse groep Europese stakeholders die zich met cyberbeveiligingstechnologie bezighouden, wordt betrokken. De kennissamenleving moet onderzoeksorganen, industrieën en de publieke sector omvatten. De kennissamenleving moet input leveren voor de activiteiten van het kenniscentrum, voor het meerjarige werkprogramma en voor het jaarlijkse werkprogramma, met name via de strategische adviesgroep. De kennissamenleving moet ook profiteren van de gemeenschapsvormende activiteiten van het kenniscentrum en het netwerk, maar mag verder voorkeursbehandeling krijgen bij oproepen tot het indienen van voorstellen en aanbestedingen. De kennissamenleving moet bestaan uit collectieve organen en organisaties. Tegelijkertijd moeten het kenniscentrum en zijn organen, om te kunnen profiteren van alle deskundigheid op het gebied van cyberbeveiliging in de Unie, ook een beroep kunnen doen op de deskundigheid van natuurlijke personen als ad-hocdeskundigen.
- (35) Het kenniscentrum moet samenwerken en zorgen voor synergie met Enisa en moet relevante input krijgen van Enisa bij het bepalen van de financieringsprioriteiten.
- (36) Om tegemoet te komen aan de behoeften zowel aan de vraag- als aan de aanbodzijde van cyberbeveiliging, moet het kenniscentrum zich bij de uitvoering van zijn taak om de industrieën kennis en technische bijstand op het gebied van cyberbeveiliging te verlenen, zowel richten op ICT-producten, -processen en -diensten als op alle andere technologische producten en processen waarin cyberbeveiligingstechnologie wordt ingebouwd. Op zijn verzoek kan de overheidssector ook gebruikmaken van steun van het kenniscentrum.
- (37) Om een duurzame cyberbeveiligingsomgeving tot stand te brengen, is het belangrijk dat security by design als beginsel wordt gebruikt bij het ontwikkelen, onderhouden, exploiteren en actualiseren van infrastructuur, producten en diensten, met name door het ondersteunen van geavanceerde veilige ontwikkelingsmethoden, adequate beveiligingstests en beveiligingsaudits, door het onverwijld beschikbaar stellen van updates om bekende kwetsbaarheden of bedreigingen te verhelpen, en waar mogelijk door derden in staat te stellen updates te creëren en te verstrekken ook na het eind van de levensduur van producten. Security by design moet tijdens de gehele levensduur van ICT-producten, -diensten of -processen worden gewaarborgd door middel van ontwikkelingsprocessen die constant evolueren om het risico op schade door kwaadwillig gebruik te verminderen.

- (38) Terwijl het kenniscentrum en het netwerk moeten streven naar meer synergie en coördinatie tussen de civiele en de militaire cyberbeveiligingsindustrie, moeten de conform deze verordening door Horizon Europa gefinancierde projecten worden uitgevoerd overeenkomstig Verordening (EU) 2021/695, waarin is bepaald dat onderzoeks- en innovatieactiviteiten in het kader van Horizon Europa exclusief op civiele toepassingen moeten zijn gericht.
- (39) Deze verordening heeft voornamelijk betrekking op civiele aangelegenheden, maar bij de activiteiten van de lidstaten op grond van deze verordening kan rekening worden gehouden met de specifieke kenmerken van de lidstaten wanneer het cyberbeveiligingsbeleid wordt gevoerd door autoriteiten die zowel civiele als militaire taken uitvoeren, moet naar complementariteit worden gestreefd en moet overlapping met defensiegerelateerde financieringsinstrumenten worden vermeden.
- (40) Deze verordening moet ervoor zorgen dat de aansprakelijkheid en de transparantie van het kenniscentrum en de ondernemingen die financiering ontvangen wordt gewaarborgd, overeenkomstig de relevante programmaverordeningen.
- (41) De uitvoering van uitrolprojecten, met name uitrolprojecten met betrekking tot infrastructuur en capaciteiten die op Unieniveau of via een gezamenlijke aanbestedingsprocedure worden uitgevoerd, kan in verschillende uitvoeringsfasen worden verdeeld, zoals afzonderlijke aanbestedingen voor het ontwerp van de architectuur van hardware en software, de productie ervan en de werking en het onderhoud ervan, waarbij bedrijven elk slechts in één fase kunnen deelnemen, in voorkomend geval met de eis dat de begunstigen in een of meer van die fasen aan bepaalde voorwaarden wat betreft Europese eigendom of zeggenschap voldoen.
- (42) Enisa moet, gezien zijn deskundigheid op het gebied van cyberbeveiliging en zijn mandaat als referentiepunt voor advies en deskundigheid ter zake voor de instellingen, organen en instanties van de Unie en voor betrokken stakeholders in de Unie, en gezien de inputs die het dankzij zijn taken verzamelt, een actieve rol spelen in de activiteiten van het kenniscentrum, waaronder de ontwikkeling van de agenda, en kan daarbij dubbel werk voorkomen, in het bijzonder dankzij zijn rol als permanent waarnemer in de raad van bestuur van het kenniscentrum. Wat de opstelling van de agenda, het jaarlijkse werkprogramma en het meerjarige werkprogramma betreft, moeten de uitvoerend directeur van het kenniscentrum en de raad van bestuur rekening houden met alle strategische adviezen en bijdragen van Enisa in dit verband, overeenkomstig het door de raad van bestuur vastgestelde reglement van orde.
- (43) Indien zij een financiële bijdrage uit de algemene begroting van de Unie ontvangen, moeten de nationale coördinatiecentra en de entiteiten die deel uitmaken van de kennisgemeenschap, bekendmaken dat hun respectieve activiteiten in het kader van deze verordening worden ondernomen.
- (44) De kosten die voortvloeien uit de oprichting en de administratieve en coördinatieactiviteiten van het kenniscentrum moeten door de Unie en door de lidstaten worden gefinancierd, in verhouding tot de vrijwillige bijdragen van de lidstaten aan gemeenschappelijke optredens. Om dubbele financiering te voorkomen, mogen deze activiteiten niet tegelijkertijd in aanmerking komen voor een bijdrage uit andere programma's van de Unie.
- (45) De raad van bestuur, die moet zijn samengesteld uit vertegenwoordigers van de lidstaten en van de Commissie, moet de algemene richting van de werkzaamheden van het kenniscentrum vaststellen en moet garanderen dat het kenniscentrum zijn taken overeenkomstig deze verordening uitvoert. De Raad van bestuur moet de agenda aannemen.
- (46) De raad van bestuur moet de noodzakelijke bevoegdheden toegewezen krijgen voor de vaststelling van de begroting van het kenniscentrum. Hij moet de uitvoering van de begroting controleren, passende financiële regels vaststellen, en transparante werkprocedures voor besluitvorming door het kenniscentrum opstellen, met inbegrip van de vaststelling van het jaarlijkse werkprogramma en het meerjarige werkprogramma overeenkomstig de agenda. De raad van bestuur moet tevens zijn reglement van orde vaststellen, de uitvoerend directeur benoemen en besluiten nemen over de verlenging of beëindiging van de ambtstermijn van de uitvoerend directeur.
- (47) De raad van bestuur moet toezicht houden op de strategische en de uitvoerende activiteiten van het kenniscentrum en de afstemming daartussen waarborgen. In zijn jaarverslag moet het kenniscentrum speciale aandacht besteden aan de strategische doelstellingen die het heeft gehaald en indien nodig voorstellen doen voor verdere verbeteringen van de verwezenlijking van die strategische doelstellingen.
- (48) Ter wille van de goede en doeltreffende werking van het kenniscentrum moeten de Commissie en de lidstaten erop toezien dat de personen die worden benoemd tot lid van de raad van bestuur over de nodige professionele deskundigheid en ervaring op functionele gebieden beschikken. De Commissie en de lidstaten dienen zich tevens in te spannen om het verloop onder hun respectieve vertegenwoordigers in de raad van bestuur te beperken teneinde de continuïteit van zijn werkzaamheden zeker te stellen.

- (49) Gezien de specifieke status en verantwoordelijkheid van het kenniscentrum voor de uitvoering van de fondsen van de Unie, met name die van Horizon Europa en het programma Digitaal Europa, moet de Commissie in de raad van bestuur 26 % van het totale aantal stemmen hebben wat betreft besluiten die betrekking hebben op Uniemiddelen, teneinde de toegevoegde Uniewaarde van die besluiten te maximaliseren en tegelijkertijd de rechtmatigheid van die besluiten en de afstemming ervan op de prioriteiten van de Unie te waarborgen.
- (50) Voor een goede werking van het kenniscentrum is het noodzakelijk dat de uitvoerend directeur op transparante wijze wordt benoemd op basis van verdiensten, aantoonbare bestuurlijke en leidinggevende vaardigheden, en bekwaamheid en ervaring die relevant is voor cyberbeveiliging; daarnaast dient de uitvoerend directeur zijn taken op volledig onafhankelijke wijze uit te voeren.
- (51) Het kenniscentrum moet beschikken over een strategische adviesgroep als adviesorgaan. De strategische adviesgroep moet advies verstrekken op basis van een regelmatige dialoog tussen het kenniscentrum en de kennisgemeenschap, die moet bestaan uit de vertegenwoordigers van de particuliere sector, consumentenorganisaties, de academische wereld en andere betrokken stakeholders. De strategische adviesgroep moet zich richten op kwesties die relevant zijn voor de stakeholders en deze onder de aandacht van de raad van bestuur en de uitvoerend directeur brengen. De taken van de strategische adviesgroep moeten onder meer bestaan in het verstrekken van advies over de agenda, het jaarlijkse werkprogramma en het meerjarige werkprogramma. De strategische adviesgroep moet een evenwichtige vertegenwoordiging van de verschillende stakeholders omvatten, met bijzondere aandacht voor de vertegenwoordiging van kmo's, om ervoor te zorgen dat stakeholders passend in de werkzaamheden van het kenniscentrum zijn vertegenwoordigd.
- (52) De bijdragen van de lidstaten aan de middelen van het kenniscentrum kunnen financieel of in natura zijn. Financiële bijdragen kunnen bijvoorbeeld bestaan uit een door een lidstaat aan een begunstigde in die lidstaat gegeven subsidie, ter aanvulling van de financiële steun van de Unie aan een project in het kader van het jaarlijkse werkprogramma. Van bijdragen in natura is meestal sprake indien een entiteit van een lidstaat zelf de begunstigde van financiële steun van de Unie is. Indien de Unie bijvoorbeeld een activiteit van een nationaal coördinatiecentrum voor 50 % subsidieert, worden de resterende kosten van de activiteit als een bijdrage in natura geboekt. Ook indien een entiteit van een lidstaat financiële steun van de Unie ontvangt voor het creëren of verbeteren van infrastructuur die door de belanghebbenden zal worden gedeeld overeenkomstig het jaarlijkse werkprogramma, worden de desbetreffende niet-gesubsidieerde kosten als bijdragen in natura geboekt.
- (53) Overeenkomstig de relevante bepalingen van Gedelegeerde Verordening (EU) 2019/715 inzake belangenconflicten, moet het kenniscentrum beschikken over regels inzake preventie, vaststelling en oplossing van, alsmede omgang met, belangenconflicten met betrekking tot zijn leden, organen en personeel, de raad van bestuur, de strategische adviesgroep en de kennisgemeenschap. De lidstaten moeten ervoor zorgen dat belangenconflicten met betrekking tot de nationale coördinatiecentra worden voorkomen, vastgesteld en opgelost conform nationaal recht. Het kenniscentrum moet verder het desbetreffende recht van de Unie inzake publieke toegang tot documenten toepassen, zoals uiteengezet in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad⁽⁹⁾. Op de verwerking van persoonsgegevens door het kenniscentrum moet Verordening (EU) 2018/1725 van het Europees Parlement en de Raad⁽¹⁰⁾ van toepassing zijn. Het kenniscentrum moet de bepalingen van Unierecht naleven die van toepassing zijn op de instellingen van de Unie, alsmede het nationaal recht inzake de behandeling van informatie, in het bijzonder de behandeling van gevoelige niet-gerubriceerde informatie en gerubriceerde EU-informatie.
- (54) De financiële belangen van de Unie en de lidstaten moeten worden beschermd met evenredige maatregelen in de gehele uitgavencyclus, onder meer op het gebied van preventie, opsporing en onderzoek van onregelmatigheden, terugvordering van verloren gegane, ten onrechte betaalde of onjuist bestede financiële middelen, en, voor zover van toepassing, met administratieve en financiële sancties overeenkomstig Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad⁽¹¹⁾ (het "Financieel Reglement").
- (55) Het kenniscentrum dient op een open en transparante manier te functioneren. Het dient alle relevante informatie tijdig ter beschikking te stellen en dient bekendheid te geven aan zijn activiteiten, onder meer door informatie- en verspreidingsactiviteiten bij het bredere publiek. Het reglement van orde van de raad van bestuur van het kenniscentrum en van de strategische adviesgroep moet openbaar worden gemaakt.

⁽⁹⁾ Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

⁽¹⁰⁾ 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).

⁽¹¹⁾ Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad van 18 juli 2018 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie, tot wijziging van Verordeningen (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 en Besluit nr. 541/2014/EU en tot intrekking van Verordening (EU, Euratom) nr. 966/2012 (PB L 193 van 30.7.2018, blz. 1).

- (56) De intern controleur van de Commissie moet ten aanzien van het kenniscentrum dezelfde bevoegdheden uitoefenen als die welke hij met betrekking tot de Commissie uitoefent.
- (57) De Commissie, de Rekenkamer en het Europees Bureau voor fraudebestrijding moeten toegang krijgen tot alle nodige informatie en alle locaties van het kenniscentrum om audits en onderzoeken uit te voeren met betrekking tot de subsidies, contracten en overeenkomsten die door het kenniscentrum zijn ondertekend.
- (58) Daar de doelstellingen van deze verordening, namelijk het vergroten van het concurrentievermogen en de capaciteiten van de Unie, het behouden en verder ontwikkelen van de technologische en industriële capaciteiten van de Unie op het gebied van cyberbeveiligingsonderzoek, het concurrerender maken van de cyberbeveiligingsbranche van de Unie en het tot concurrentievoordeel voor andere bedrijfstakken in de Unie maken van cyberbeveiliging, niet voldoende door de lidstaten alleen kunnen worden verwezenlijkt omdat de bestaande, beperkte middelen versnipperd zijn en omdat de benodigde investeringen aanzienlijk zijn, maar beter door de Unie kunnen worden verwezenlijkt omdat zo dubbel werk wordt vermeden, er een kritische massa van investeringen kan worden bereikt, de overheidsfinanciering optimaal wordt benut en een hoog niveau van cyberbeveiliging wordt bevorderd in alle lidstaten, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie (VEU) neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstellingen te verwezenlijken,

HEBLEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

Algemene bepalingen en beginselen van het kenniscentrum en het netwerk

Artikel 1

Onderwerp en toepassingsgebied

1. Bij deze verordening worden het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (het "kenniscentrum") en het netwerk van nationale coördinatiecentra (het "netwerk") opgericht. Zij stelt regels vast voor de aanwijzing van nationale coördinatiecentra en regels voor de oprichting van de kennissamenleving voor cyberbeveiliging (de "kennissamenleving").
2. Het kenniscentrum speelt een essentiële rol in de uitvoering van het onderdeel cyberbeveiliging van het programma Digitaal Europa, met name wat betreft acties met betrekking tot artikel 6 van Verordening (EU) 2021/694, en draagt bij tot de uitvoering van Horizon Europa, met name wat betreft afdeling 3.1.3. van pijler II van bijlage I bij Besluit (EU) 2021/764 van de Raad ⁽¹²⁾.
3. De lidstaten dragen gezamenlijk bij tot de werkzaamheden van het kenniscentrum en het netwerk.
4. Deze verordening laat de bevoegdheden van de lidstaten betreffende openbare veiligheid, defensie, nationale veiligheid en activiteiten van de staat op strafrechtelijk gebied onverlet.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) "cyberbeveiliging": de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen;
- 2) "netwerk- en informatiesysteem": een netwerk- en informatiesysteem als gedefinieerd in artikel 4, punt 1, van Richtlijn (EU) 2016/1148;
- 3) "cyberbeveiligingsproducten, -diensten en -processen": commerciële en niet-commerciële ICT-producten, -diensten of -processen met als specifiek doel netwerk- en informatiesystemen te beschermen of te zorgen voor de vertrouwelijkheid, integriteit en toegankelijkheid van gegevens die worden verwerkt of opgeslagen in netwerk- en informatiesystemen, en voor de cyberbeveiliging van de gebruikers van die systemen, en andere door cyberdreigingen getroffen personen;
- 4) "cyberdreiging": elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden;

⁽¹²⁾ Besluit (EU) 2021/764 van de Raad van 10 mei 2021 tot vaststelling van het specifieke programma tot uitvoering van Horizon Europa — het kaderprogramma voor onderzoek en innovatie, en tot intrekking van Besluit 2013/743/EU (PB L 167 I van 12.5.2021, blz. 1).

- 5) “gezamenlijke actie”: een in het jaarlijkse werkprogramma opgenomen actie die financiële steun van de Unie ontvangt uit Horizon Europa, het programma Digitaal Europa of andere Unieprogramma's, alsmede financiële steun of steun in natura van een of meer lidstaten, en die wordt uitgevoerd via projecten waarbij begunstigen zijn betrokken die zijn gevestigd in en financiële steun of steun in natura ontvangen van die lidstaten;
- 6) “bijdrage in natura”: de in aanmerking komende kosten die worden gemaakt door nationale coördinatiecentra en andere publieke entiteiten wanneer zij deelnemen aan projecten die op grond van deze verordening worden gefinancierd, wanneer die kosten niet worden gefinancierd door een bijdrage van de Unie of door financiële bijdragen van de lidstaten;
- 7) “Europese digitale-innovatiehub”: een Europese digitale-innovatiehub als gedefinieerd in artikel 2, punt e), van Verordening (EU) 2021/694;
- 8) “agenda”: een integrale en duurzame strategie voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging, waarin strategische aanbevelingen voor de ontwikkeling en groei van de Europese industriële, technologische en onderzoekssector op het gebied van cyberbeveiliging en strategische prioriteiten voor de activiteiten van het kenniscentrum zijn opgenomen en die niet bindend is ten aanzien van de besluiten die over de jaarlijkse werkprogramma's moeten worden genomen;
- 9) “technische bijstand”: het bijstaan door het kenniscentrum van de nationale coördinatiecentra of de kennisgemeenschap bij de uitvoering van hun taken, door kennis te verschaffen of de toegang tot deskundigheid op het gebied van onderzoek, technologie en industrie met betrekking tot cyberbeveiliging te vergemakkelijken, netwerkvorming te faciliteren, bewustwording te verhogen en samenwerking te bevorderen, of het bijstaan door het kenniscentrum samen met de nationale coördinatiecentra van stakeholders met betrekking tot de voorbereiding van projecten met betrekking tot de opdracht van het kenniscentrum en het netwerk en de doelstellingen van het kenniscentrum.

Artikel 3

Oprichting van het kenniscentrum en het netwerk

1. De opdracht van het kenniscentrum en het netwerk is de Unie te helpen:
 - a) om haar leiderschap en strategische autonomie op het gebied van cyberbeveiliging te versterken door het behoud en de ontwikkeling van de onderzoeks-, academische, maatschappelijke, technologische en industriële capaciteiten en vermogens van de Unie op het gebied van cyberbeveiliging die nodig zijn om het vertrouwen en de veiligheid te vergroten, met inbegrip van de betrouwbaarheid, integriteit en toegankelijkheid van gegevens in de digitale eengemaakte markt;
 - b) bij het ondersteunen van technologische capaciteiten, vermogens en vaardigheden in de Unie met betrekking tot de weerbaarheid en betrouwbaarheid van de infrastructuur van netwerk- en informatiesystemen, met inbegrip van vitale infrastructuur en algemeen gebruikte hardware en software in de Unie, en
 - c) om het mondiale concurrentievermogen van de cyberbeveiligingssector van de Unie te vergroten, te zorgen voor hoge normen op het gebied van cyberbeveiliging in de hele Unie, en van cyberbeveiliging een concurrentievoordeel voor andere industrieën in de Unie te maken.
2. In voorkomend geval voeren het kenniscentrum en het netwerk hun taken uit in samenwerking met Enisa en de kennisgemeenschap.
3. Het kenniscentrum gebruikt de betreffende financiële middelen van de Unie op zodanige wijze dat ze bijdragen aan de in lid 1 bedoelde opdracht, in overeenstemming met de wetgevingshandelingen tot vaststelling van de relevante programma's, met name Horizon Europa en het programma Digitaal Europa.

Artikel 4

Doelstellingen van het kenniscentrum

1. Het kenniscentrum heeft als algemene doelstelling het bevorderen van onderzoek, innovatie en uitrol op het gebied van cyberbeveiliging teneinde de in artikel 3 opgenomen opdracht te vervullen.
2. De specifieke doelstellingen van het kenniscentrum zijn:
 - a) het verbeteren van de capaciteiten, vermogens, kennis en infrastructuur op het gebied van cyberbeveiliging ten dienste van het bedrijfsleven, met name kmo's, onderzoeksgemeenschappen, de overheidssector en het maatschappelijk middenveld, voor zover van toepassing;
 - b) het bevorderen van de weerbaarheid op het gebied van cyberbeveiliging, de acceptatie van beste praktijken op het gebied van cyberbeveiliging, het beginsel van security by design en de certificering van de beveiliging van digitale producten en diensten, op een manier die de inspanningen van andere publieke entiteiten aanvult;
 - c) bijdragen aan een sterk Europees cyberbeveiligingsecosysteem dat alle betrokken stakeholders samenbrengt.

3. Het kenniscentrum voert de in lid 2 bedoelde specifieke doelstellingen uit door:
- a) het vaststellen van strategische aanbevelingen voor onderzoek, innovatie en uitrol op het gebied van cyberbeveiliging in overeenstemming met het recht van de Unie en het vaststellen van strategische prioriteiten voor de activiteiten van het kenniscentrum;
 - b) het uitvoeren van acties in het kader van de betreffende financieringsprogramma's van de Unie in overeenstemming met de relevante werkprogramma's en de wetgevingshandelingen van de Unie tot vaststelling van die financieringsprogramma's;
 - c) het bevorderen van samenwerking en coördinatie tussen de nationale coördinatiecentra en met en binnen de kennisgemeenschap, en
 - d) indien van toepassing en wenselijk, het verwerven en exploiteren van ICT-infrastructuur en -diensten waar dat nodig is voor de uitvoering van de in artikel 5 vervatte taken en in overeenstemming met de respectieve werkprogramma's van artikel 5, lid 3, punt b).

Artikel 5

Taken van het kenniscentrum

1. Ter vervulling van zijn opdracht en doelstellingen voert het kenniscentrum de volgende taken uit:
 - a) strategische taken en
 - b) uitvoerende taken.
2. De strategische taken als bedoeld in lid 1, punt a), bestaan uit:
 - a) het ontwikkelen van en toezien op de uitvoering van de agenda;
 - b) via de agenda en het meerjarige werkprogramma, overlapping van activiteiten met Enisa vermijgend en rekening houdend met de noodzaak om synergie tot stand te brengen tussen cyberbeveiliging en andere onderdelen van Horizon Europa en het programma Digitaal Europa:
 - i) het vaststellen van prioriteiten voor het werk van het kenniscentrum inzake:
 - 1) de bevordering van onderzoek en innovatie op het gebied van cyberbeveiliging gedurende de gehele innovatiecyclus, en de uitrol van dat onderzoek en die innovatie;
 - 2) de ontwikkeling van capaciteiten, vermogen en infrastructuur op het gebied van industrie, technologie en onderzoek met betrekking tot cyberbeveiliging;
 - 3) de verbetering van de vaardigheden en competenties op het gebied van cyberbeveiliging en technologie in industrie, technologie en onderzoek en op alle betreffende onderwijsniveaus, waarbij genderevenwicht wordt ondersteund;
 - 4) de uitrol van cyberbeveiligingsproducten, -diensten en -processen;
 - 5) de ondersteuning van de acceptatie door de markt van cyberbeveiligingsproducten, -diensten en -processen die bijdragen aan de in artikel 3 bedoelde opdracht;
 - 6) de ondersteuning van de acceptatie en integratie van geavanceerde cyberbeveiligingsproducten, -diensten en -processen door overheidsinstanties op hun verzoek, door het bedrijfsleven aan de vraagzijde en door andere gebruikers;
 - ii) het ondersteunen van de cyberbeveiligingssector, met name kmo's, met het oog op het vergroten van de excellentie, de capaciteiten en het concurrentievermogen van de Unie op het gebied van cyberbeveiliging, onder meer met het oog op de aansluiting op potentiële markten en uitrolmogelijkheden, en het aantrekken van investeringen, en
 - iii) het verlenen van steun en technische bijstand aan starters, kmo's, micro-ondernemingen, verenigingen, individuele deskundigen en civic technology-projecten op het gebied van cyberbeveiliging;
 - c) het zorgen voor synergie tussen en samenwerking met de betrokken instellingen, organen en instanties van de Unie, met name Enisa, waarbij overlapping van activiteiten met die instellingen, organen en instanties van de Unie wordt vermeden;
 - d) het coördineren van de nationale coördinatiecentra via het netwerk en het zorgen voor een regelmatige uitwisseling van deskundigheid;

- e) het verstrekken van deskundig advies aan de lidstaten, op hun verzoek, over industrie, technologie en onderzoek op het gebied van cyberbeveiliging, onder meer met betrekking tot aanbestedingen en de uitrol van technologieën;
- f) het faciliteren van samenwerking en het delen van deskundigheid tussen alle betrokken stakeholders, met name tussen leden van de kennisgemeenschap;
- g) het bijwonen van uniale, nationale en internationale conferenties, beurzen en fora die verband houden met de opdracht, doelstellingen en taken van het kenniscentrum, met het oog op het delen van standpunten en het uitwisselen van beste praktijken op dit gebied met andere deelnemers;
- h) het faciliteren van het gebruik van de resultaten van onderzoeks- en innovatieprojecten in het kader van acties in verband met de ontwikkeling van cyberbeveiligingsproducten, -diensten en -processen, waarbij ernaar wordt gestreefd versnippering en dubbel werk te voorkomen en goede cyberbeveiligingspraktijken, -diensten en -processen worden verspreid, met name die welke door kmo's zijn ontwikkeld en die welke gebruikmaken van opensourcesoftware.

3. De in lid 1, punt b), bedoelde uitvoeringstaken bestaan uit:

- a) het coördineren en beheren van de werkzaamheden van het netwerk en de kennisgemeenschap teneinde de in artikel 3 omschreven opdracht te verwezenlijken, met name door het ondersteunen van starters, kleine en middelgrote ondernemingen, micro-ondernemingen, verenigingen en civic technology-projecten in de Unie op het gebied van cyberbeveiliging, en het vergemakkelijken van hun toegang tot deskundigheid, financiering, investeringen en markten;
- b) het opstellen en uitvoeren, overeenkomstig de agenda en het meerjarige werkprogramma, van het jaarlijkse werkprogramma met betrekking tot de onderdelen cyberbeveiliging van:
 - i) het programma Digitaal Europa, met name acties die verband houden met artikel 6 van Verordening (EU) 2021/694;
 - ii) gezamenlijke acties die steun ontvangen in het kader van de bepalingen die verband houden met cyberbeveiliging in Horizon Europa, met name wat betreft afdeling 3.1.3. van pijler II van bijlage I bij Besluit (EU) 2021/764, overeenkomstig het meerjarige werkprogramma en het strategische planningsproces van Horizon Europa, en
 - iii) andere programma's indien de relevante wetgevingshandelingen van de Unie daarin voorzien;
- c) het ondersteunen, waar nodig, van de verwezenlijking van specifieke doelstelling 4, "geavanceerde digitale vaardigheden", als bedoeld in artikel 7 van Verordening (EU) 2021/694, in samenwerking met de Europese digitale-innovatie-hubs;
- d) het verstrekken van deskundig advies over industrie, technologie en onderzoek op het gebied van cyberbeveiliging aan de Commissie wanneer deze de ontwerpwerkprogramma's opstelt overeenkomstig artikel 13 van Besluit (EU) 2021/764;
- e) het uitvoeren of mogelijk maken van de uitrol van ICT-infrastructuur en het faciliteren van de verwerving van dergelijke infrastructuur, ten behoeve van de samenleving, de industrie en de overheidssector, op verzoek van de lidstaten, onderzoeksgemeenschappen en aanbieders van essentiële diensten, onder meer via bijdragen van de lidstaten en Uniefinanciering voor gezamenlijke acties, in overeenstemming met de agenda, het jaarlijkse werkprogramma en het meerjarige werkprogramma;
- f) het bewustmaken van de opdracht van het kenniscentrum en het netwerk en van de doelstellingen en taken van het kenniscentrum;
- g) zonder afbreuk te doen aan het civiele karakter van de projecten die uit Horizon Europa worden gefinancierd, en in overeenstemming met Verordeningen (EU) 2021/695 en (EU) 2021/694, het versterken van synergie en het verbeteren van coördinatie tussen de civiele en de militaire aspecten van cyberbeveiliging, door het vergemakkelijken van de uitwisseling van:
 - i) kennis en informatie met betrekking tot technologieën en toepassingen voor tweërlei gebruik,
 - ii) resultaten, vereisten en beste praktijken, en
 - iii) informatie over de prioriteiten van de betreffende programma's van de Unie.

4. Het kenniscentrum voert de in lid 1 bedoelde taken uit in nauwe samenwerking met het netwerk.

5. Overeenkomstig artikel 6 van Verordening (EU) 2021/695 en onder voorbehoud van een bijdrageovereenkomst als gedefinieerd in artikel 2, punt 18), van het Financieel Reglement, kan het kenniscentrum worden belast met de uitvoering van de niet door de lidstaten medegefinancierde onderdelen cyberbeveiliging in het kader van Horizon Europa, met name wat betreft afdeling 3.1.3. van pijler II van bijlage I bij Besluit (EU) 2021/764.

Artikel 6

Aanwijzing van nationale coördinatiecentra

1. Elke lidstaat wijst uiterlijk op 29 december 2021 een entiteit die de in lid 5 vastgestelde criteria vervult aan om op te treden als nationaal coördinatiecentrum voor de toepassing van deze verordening. Elke lidstaat stelt de raad van bestuur onverwijld in kennis van de aanwijzing van die entiteit. Een dergelijke entiteit kan een entiteit zijn die reeds in die lidstaat is gevestigd.

De in de eerste alinea van dit lid bepaalde termijn wordt verlengd met de periode waarin de Commissie het in lid 2 bedoelde advies dient uit te brengen.

2. Een lidstaat kan de Commissie te allen tijde om advies verzoeken over de vraag of de entiteit die de lidstaat heeft aangewezen of voornemens is aan te wijzen als nationaal coördinatiecentrum de nodige capaciteit heeft om de middelen voor de verwezenlijking van de in deze verordening vastgelegde opdracht en doelstellingen te beheren. De Commissie brengt binnen drie maanden na het verzoek van de lidstaat advies uit aan die lidstaat.

3. Uiterlijk drie maanden nadat een entiteit als bedoeld in lid 1 door een lidstaat is gemeld, registreert de raad van bestuur deze entiteit op basis van die melding als nationaal coördinatiecentrum. Het kenniscentrum maakt de lijst van aangewezen nationale coördinatiecentra bekend.

4. Een lidstaat kan voor de toepassing van deze verordening te allen tijde een nieuwe entiteit als nationaal coördinatiecentrum aanwijzen. De leden 1, 2 en 3 zijn van toepassing op de aanwijzing van nieuwe entiteiten.

5. Het nationale coördinatiecentrum is een openbare instelling of een entiteit waarin de lidstaat een meerderheidsbelang aanhoudt, die openbare diensttaken verricht krachtens het nationale recht, onder meer door middel van bevoegdheidsdelegatie, en beschikt over de capaciteit om het kenniscentrum en het netwerk te ondersteunen bij de uitvoering van hun opdracht als omschreven in artikel 3 van deze verordening. Het beschikt over, of heeft toegang tot, onderzoeks- en technologische deskundigheid op het gebied van cyberbeveiliging. Het beschikt over de capaciteit om effectief in dialoog te gaan en samen te werken met de industrie, de overheidssector, de academische en de onderzoeksgemeenschap, en de burgers, alsook met de overeenkomstig Richtlijn (EU) 2016/1148 aangewezen autoriteiten.

6. Een nationaal coördinatiecentrum kan te allen tijde verzoeken dat wordt erkend dat het de nodige capaciteit heeft om middelen te beheren teneinde de in deze verordening vastgestelde opdracht en doelstellingen te verwezenlijken, overeenkomstig Verordeningen (EU) 2021/695 en (EU) 2021/694. Binnen drie maanden na een dergelijk verzoek beoordeelt de Commissie of dat nationale coördinatiecentrum over dergelijke capaciteit beschikt en neemt zij een besluit.

Indien de Commissie een lidstaat een positief advies heeft verstrekt overeenkomstig de procedure van lid 2, wordt dat advies beschouwd als een besluit tot erkenning dat de desbetreffende entiteit over de nodige capaciteit beschikt voor de toepassing van dit lid.

Uiterlijk op 29 augustus 2021 stelt de Commissie, na overleg met de raad van bestuur, richtsnoeren vast inzake de beoordeling bedoeld in de eerste alinea, met inbegrip van een specificatie van de voorwaarden voor erkenning en de wijze waarop adviezen worden uitgebracht en beoordelingen worden uitgevoerd.

Vóór het uitbrengen van het in lid 2 bedoelde advies en het nemen van het in de eerste alinea van dit lid bedoelde besluit houdt de Commissie rekening met de door het verzoekende nationale coördinatiecentrum verstrekte informatie en documentatie.

Elk besluit om een nationaal coördinatiecentrum niet te erkennen als beschikkend over de nodige capaciteit om middelen te beheren teneinde de in deze verordening vastgestelde opdracht en doelstellingen te verwezenlijken wordt afgewezen, wordt afdoende gemotiveerd, met vermelding van de vereisten waaraan het verzoekende nationale coördinatiecentrum nog niet voldoet en die het besluit tot niet-erkenning rechtvaardigen. Elk nationaal coördinatiecentrum waarvan het verzoek tot erkenning is afgewezen, kan zijn verzoek te allen tijde opnieuw indienen met aanvullende informatie.

De lidstaten stellen de Commissie in kennis van wijzigingen inzake het nationale coördinatiecentrum, zoals de samenstelling van het nationale coördinatiecentrum, de juridische vorm van het nationale coördinatiecentrum of andere relevante aspecten die van invloed zijn op zijn vermogen om middelen te beheren teneinde aan de in deze verordening vastgestelde opdracht en doelstellingen te voldoen. Bij ontvangst van dergelijke informatie kan de Commissie een besluit om de erkenning van het nationaal coördinatiecentrum als beschikkend over de nodige capaciteit om middelen te beheren, te verlenen of niet te verlenen, dienovereenkomstig herzien.

7. Het netwerk bestaat uit alle nationale coördinatiecentra die door de lidstaten bij de raad van bestuur zijn aangemeld.

Artikel 7

Taken van de nationale coördinatiecentra

1. De nationale coördinatiecentra verrichten de volgende taken:
 - a) optreden als contactpunt op nationaal niveau voor de kennissamenleving ter ondersteuning van het kenniscentrum bij de verwezenlijking van zijn opdracht en doelstellingen, in het bijzonder bij de coördinatie van de kennissamenleving door het coördineren van de leden van de kennissamenleving in hun lidstaten;
 - b) verstrekken van deskundig advies en actief bijdragen aan de strategische taken als bedoeld in artikel 5, lid 2, rekening houdend met de relevante nationale en regionale uitdagingen op het gebied van cyberbeveiliging in verschillende sectoren;
 - c) bevorderen, stimuleren en vergemakkelijken op nationaal niveau van de deelname van het maatschappelijk middenveld, de industrie, met name starters en kmo's, de academische en onderzoeksgemeenschap en andere stakeholders aan grensoverschrijdende projecten en aan acties op het gebied van cyberbeveiliging die uit de betreffende Unieprogramma's gefinancierd worden;
 - d) verlenen van technische bijstand aan stakeholders door hen te ondersteunen in de aanvraagfase voor door het kenniscentrum beheerde projecten met betrekking tot zijn opdracht en doelstellingen, en met volledige inachtneming van de regels van goed financieel beheer, in het bijzonder wat betreft belangenconflicten;
 - e) streven naar synergieën met relevante activiteiten op nationaal, regionaal en lokaal niveau, zoals nationaal beleid inzake onderzoek, ontwikkeling en innovatie op het gebied van cyberbeveiliging, met name het beleid dat in de nationale cyberbeveiligingsstrategieën is uiteengezet;
 - f) uitvoeren van specifieke acties waaraan het kenniscentrum subsidies heeft toegekend, onder meer door middel van financiële steun aan derden overeenkomstig artikel 204 van het Financieel Reglement onder de in de betreffende subsidieovereenkomsten genoemde voorwaarden;
 - g) onverlet de bevoegdheden van de lidstaten op het gebied van onderwijs en rekening houdend met de betreffende taken van Enisa, overleggen met de nationale autoriteiten over mogelijke bijdragen aan de bevordering en verspreiding van onderwijsprogramma's op het gebied van cyberbeveiliging;
 - h) bevorderen en verspreiden van de betreffende resultaten van de werkzaamheden van het netwerk, de kennissamenleving en het kenniscentrum op nationaal, regionaal of lokaal niveau;
 - i) beoordelen van verzoeken van een in dezelfde lidstaat als het nationale coördinatiecentrum gevestigde entiteit om deel te gaan uitmaken van de kennissamenleving;
 - j) pleiten voor en bevorderen van de betrokkenheid van relevante entiteiten bij de activiteiten van het kenniscentrum, het netwerk en de kennissamenleving en, indien nodig, toezicht houden op de mate van betrokkenheid bij en het bedrag aan publieke financiële steun voor onderzoek, ontwikkeling en uitrol op het gebied van cyberbeveiliging.
2. Voor de toepassing van punt f) van lid 1 van dit artikel kan de financiële steun aan derden in een van de in artikel 125 van het Financieel Reglement genoemde vormen van bijdragen van de Unie worden verleend, ook in de vorm van vaste bedragen.
3. Op basis van een besluit als bedoeld in artikel 6, lid 6, van deze verordening kunnen nationale coördinatiecentra overeenkomstig artikel 195, eerste alinea, punt d), van het Financieel Reglement van de Unie een subsidie ontvangen voor de uitvoering van de in dit artikel omschreven taken.
4. De nationale coördinatiecentra werken waar nodig samen via het netwerk.

Artikel 8

De kennissamenleving voor cyberbeveiliging

1. De kennissamenleving draagt bij aan de in artikel 3 vastgelegde opdracht van het kenniscentrum en het netwerk, en vergroot, deelt en verspreidt de deskundigheid over cyberbeveiliging in de hele Unie.

2. De kennisgemeenschap bestaat uit de industrie, ook kmo's, academische en onderzoeksorganisaties, andere betrokken verenigingen uit het maatschappelijk middenveld en, in voorkomend geval, de betrokken Europese standaardiseringsorganisaties, publieke en andere entiteiten die zich bezighouden met operationele en technische cyberbeveiligingsaanlegenheden, en, in voorkomend geval, uit stakeholders in sectoren die een belang hebben bij cyberbeveiliging en geconfronteerd worden met cyberbeveiligingsuitdagingen. De kennisgemeenschap brengt de voornaamste stakeholders wat betreft technologische, industriële, wetenschappelijke en onderzoekscapaciteiten op het gebied van cyberbeveiliging in de Unie bijeen. Nationale coördinatiecentra, Europese digitale-innovatiehubs indien van toepassing en instellingen, organen en instanties van de Unie met relevante deskundigheid zoals Enisa worden erbij betrokken.

3. Alleen in de lidstaten gevestigde entiteiten kunnen als lid van de kennisgemeenschap worden geregistreerd. Zij moeten aantonen dat zij kunnen bijdragen aan de opdracht en moeten beschikken over deskundigheid op het gebied van cyberbeveiliging op ten minste een van de volgende terreinen:

- a) wetenschap, onderzoek of innovatie;
- b) industriële of productontwikkeling;
- c) opleiding en onderwijs;
- d) informatiebeveiliging of respons op incidenten;
- e) ethiek;
- f) formele en technische normalisatie en specificaties.

4. Het kenniscentrum registreert op verzoek entiteiten als lid van de kennisgemeenschap nadat het nationaal coördinatiecentrum van de lidstaat waar die entiteiten zijn gevestigd, een beoordeling heeft verricht om te bevestigen dat die entiteiten voldoen aan de criteria van lid 3 van dit artikel. Bij die beoordeling wordt ook rekening gehouden met elke relevante nationale beoordeling op grond van veiligheidsoverwegingen die is verricht door de bevoegde nationale autoriteiten. Een dergelijke registratie is niet in de tijd beperkt, maar kan te allen tijde door het kenniscentrum worden ingetrokken indien het betrokken nationale coördinatiecentrum van oordeel is dat de betrokken entiteit niet langer aan de criteria van lid 3 van dit artikel voldoet of onder artikel 136 van het Financieel Reglement valt, of om gerechtvaardigde veiligheidsoverwegingen. Indien het lidmaatschap van de kennisgemeenschap om veiligheidsredenen wordt ingetrokken, is het besluit tot intrekking proportioneel en gemotiveerd. De nationale coördinatiecentra streven naar een evenwichtige vertegenwoordiging van stakeholders in de kennisgemeenschap en stimuleren actief de deelname eraan, met name van kmo's.

5. De nationale coördinatiecentra worden aangemoedigd om via het netwerk samen te werken ter harmonisering van de wijze waarop zij de in lid 3 bepaalde criteria toepassen en van de procedures voor de beoordeling en registratie van de in lid 4 bedoelde entiteiten.

6. Het kenniscentrum registreert de bevoegde instellingen, organen en instanties van de Unie als lid van de kennisgemeenschap, nadat het een beoordeling heeft verricht om te bevestigen dat die instelling, dat orgaan of die instantie van de Unie aan de criteria van lid 3 van dit artikel voldoet. Een dergelijke registratie is niet in de tijd beperkt, maar kan te allen tijde door het kenniscentrum worden ingetrokken indien het van oordeel is dat de instelling, het orgaan of de instantie van de Unie niet langer aan de criteria van lid 3 van dit artikel voldoet of onder artikel 136 van het Financieel Reglement valt.

7. Vertegenwoordigers van de instellingen, organen en instanties van de Unie kunnen aan de werkzaamheden van de kennisgemeenschap deelnemen.

8. Een entiteit die als lid van de kennisgemeenschap is geregistreerd, wijst haar respectieve vertegenwoordigers aan om een efficiënte dialoog te waarborgen. Deze vertegenwoordigers beschikken over deskundigheid op het gebied van onderzoek, technologie of industrie met betrekking tot cyberbeveiliging. De vereisten kunnen nader worden gespecificeerd door de raad van bestuur, zonder dat de entiteiten bij de aanwijzing van hun vertegenwoordigers onnodig worden beperkt.

9. De kennisgemeenschap verstrekt via haar werkgroepen en met name via de strategische adviesgroep aan de uitvoerend directeur en aan de raad van bestuur strategisch advies over de agenda, het jaarlijkse werkprogramma en het meerjarige werkprogramma, overeenkomstig het reglement van orde van de raad van bestuur.

*Artikel 9***Taken van de leden van de kennisgemeenschap**

De leden van de kennisgemeenschap:

- a) ondersteunen het kenniscentrum bij de verwezenlijking van zijn opdracht en doelstellingen, en werken daartoe nauw samen met het kenniscentrum en de nationale coördinatiecentra;
- b) nemen, waar nodig, deel aan formele of informele activiteiten en aan de werkgroepen bedoeld in artikel 13, lid 3, punt n), voor het uitvoeren van specifieke activiteiten zoals bepaald in het jaarlijkse werkprogramma, en
- c) bieden indien nodig ondersteuning aan het kenniscentrum en de nationale coördinatiecentra bij de promotie van specifieke projecten.

*Artikel 10***Samenwerking van het kenniscentrum met andere instellingen, organen en instanties van de Unie en met internationale organisaties**

1. Om samenhang en complementariteit te waarborgen en dubbel werk te voorkomen, werkt het kenniscentrum samen met de bevoegde instellingen, organen en instanties van de Unie, waaronder Enisa, de Europese Dienst voor extern optreden, het directoraat-generaal Gemeenschappelijk Centrum voor onderzoek van de Commissie, het Europees Uitvoerend Agentschap onderzoek, het Uitvoerend Agentschap Europese Onderzoeksraad en het Europees Uitvoerend Agentschap voor gezondheid en digitaal beleid opgericht bij Uitvoeringsbesluit (EU) 2021/173 van de Commissie⁽¹³⁾, de betreffende Europese digitale innovatiehubs, het Europees Centrum voor de bestrijding van cybercriminaliteit bij het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving, opgericht bij Verordening (EU) 2016/794 van het Europees Parlement en de Raad⁽¹⁴⁾, het Europees Defensieagentschap met betrekking tot de in artikel 5 van deze verordening genoemde taken, en andere bevoegde entiteiten van de Unie. Het kenniscentrum kan in voorkomend geval ook samenwerken met internationale organisaties.

2. De samenwerking als bedoeld in lid 1 van dit artikel kan in het kader van werkafspraken geschieden. Deze afspraken worden ter goedkeuring aan de raad van bestuur voorgelegd. Het delen van gerubriceerde informatie vindt plaats in het kader van administratieve regelingen die overeenkomstig artikel 36, lid 3, zijn getroffen.

*HOOFDSTUK II***Organisatie van het kenniscentrum***Artikel 11***Lidmaatschap en structuur**

1. De leden van het kenniscentrum zijn de Unie, vertegenwoordigd door de Commissie, en de lidstaten.
2. De structuur van het kenniscentrum zorgt ervoor dat de in artikel 4 omschreven doelstellingen en de in artikel 5 omschreven taken worden verwezenlijkt, en omvat:
 - a) een raad van bestuur,
 - b) een uitvoerend directeur,
 - c) een strategische adviesgroep.

⁽¹³⁾ Uitvoeringsbesluit (EU) 2021/173 van de Commissie van 12 februari 2021 tot oprichting van het Europees Uitvoerend Agentschap klimaat, milieu en infrastructuur, het Europees Uitvoerend Agentschap voor gezondheid en digitaal beleid, het Europees Uitvoerend Agentschap onderzoek, het Europees Uitvoerend Agentschap Innovatieraad en het mkb, het Uitvoerend Agentschap Europese Onderzoeksraad en het Europees Uitvoerend Agentschap voor onderwijs en culturen tot intrekking van de Uitvoeringsbesluiten 2013/801/EU, 2013/771/EU, 2013/778/EU, 2013/779/EU, 2013/776/EU en 2013/770/EU (PB L 50 van 15.2.2021, blz. 9).

⁽¹⁴⁾ Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad (PB L 135 van 24.5.2016, blz. 53).

Afdeling I

Raad van bestuur

Artikel 12

Samenstelling van de raad van bestuur

1. De raad van bestuur bestaat uit één vertegenwoordiger van elke lidstaat en twee vertegenwoordigers van de Commissie die optreden namens de Unie.
2. Elk lid van de raad van bestuur heeft een plaatsvervanger. Die plaatsvervanger vertegenwoordigt het lid in geval van diens afwezigheid.
3. De door de lidstaten benoemde leden van de raad van bestuur en hun plaatsvervangers zijn personeelsleden van de overheid in hun respectieve lidstaat, en worden benoemd op grond van hun kennis op het gebied van onderzoek, technologie en industrie op het gebied van cyberbeveiliging, hun vermogen om te zorgen voor de coördinatie van acties en standpunten met hun respectieve nationale coördinatiecentrum, of op grond van hun relevante bestuurlijke, administratieve en budgettaire vaardigheden. De Commissie benoemt haar leden van de raad van bestuur en hun plaatsvervangers op grond van hun kennis op het gebied van cyberbeveiliging, technologie of hun relevante bestuurlijke, administratieve en budgettaire vaardigheden, en van hun vermogen te zorgen voor coördinatie, synergieën en, voor zover mogelijk, gezamenlijke initiatieven tussen de verschillende sectorale of horizontale beleidsterreinen van de Unie die te maken hebben met cyberbeveiliging. De Commissie en de lidstaten spannen zich ter wille van de continuïteit van het werk van de raad van bestuur in om het verloop onder hun vertegenwoordigers in de raad van bestuur te beperken. De Commissie en de lidstaten streven naar een evenwichtige vertegenwoordiging van mannen en vrouwen in de raad van bestuur.
4. De ambtstermijn van de leden van de raad van bestuur en hun plaatsvervangers bedraagt vier jaar. Die termijn kan worden verlengd.
5. De leden van de raad van bestuur zorgen er op onafhankelijke en transparante wijze voor dat de doelstellingen, opdracht, identiteit en autonomie van het kenniscentrum worden gewaarborgd en dat de acties van het kenniscentrum consistent zijn met die opdracht en doelstellingen.
6. De raad van bestuur kan waarnemers uitnodigen om waar dit passend is deel te nemen aan zijn vergaderingen, onder wie vertegenwoordigers van relevante instellingen, organen en instanties van de Unie en de leden van de kennisgemeenschap.
7. Een vertegenwoordiger van Enisa is een permanente waarnemer in de raad van bestuur. De raad van bestuur kan een vertegenwoordiger van de strategische adviesgroep uitnodigen om zijn vergaderingen bij te wonen.
8. De uitvoerend directeur neemt deel aan de vergaderingen van de raad van bestuur, maar heeft geen stemrecht.

Artikel 13

Taken van de raad van bestuur

1. De raad van bestuur draagt de volledige verantwoordelijkheid voor de strategische koers en de werkzaamheden van het kenniscentrum, houdt toezicht op de uitvoering van zijn activiteiten en is verantwoordelijk voor alle taken die niet specifiek aan de uitvoerend directeur zijn toegewezen.
2. De raad van bestuur stelt zijn reglement van orde vast. Dat reglement van orde voorziet in specifieke procedures om belangenconflicten vast te stellen en te voorkomen, en waarborgt de vertrouwelijkheid van gevoelige informatie.
3. De raad van bestuur neemt de noodzakelijke strategische besluiten, met name met betrekking tot:
 - a) het opstellen en aannemen van de agenda en het monitoren van de uitvoering ervan;
 - b) de vaststelling, conform de beleidsprioriteiten van de Unie en de agenda, van het meerjarige werkprogramma, dat gemeenschappelijke prioriteiten op het gebied van industrie, technologie en onderzoek omvat, die gebaseerd zijn op de behoeften die de lidstaten in samenwerking met de kennisgemeenschap hebben vastgesteld en waarvoor gerichte financiële steun van de Unie vereist is, met inbegrip van belangrijke technologieën en terreinen voor de ontwikkeling van de eigen vermogens van de Unie op het gebied van cyberbeveiliging;
 - c) de vaststelling van het jaarlijkse werkprogramma voor de uitvoering van de desbetreffende fondsen van de Unie, met name de onderdelen cyberbeveiliging van Horizon Europa die vrijwillig medegefinancierd worden door de lidstaten en van het programma Digitaal Europa, overeenkomstig het meerjarige werkprogramma van het kenniscentrum en het strategische planningsproces van Horizon Europa;

- d) de vaststelling, op basis van een voorstel van de uitvoerend directeur, van de jaarrekeningen, de balans en het jaarlijkse activiteitenverslag van het kenniscentrum;
- e) de vaststelling van de specifieke financiële regels van het kenniscentrum overeenkomstig artikel 70 van het Financieel Reglement;
- f) de toewijzing, als onderdeel van het jaarlijkse werkprogramma, van de begrotingsmiddelen van de Unie aan onderwerpen voor gezamenlijke acties van de Unie en de lidstaten;
- g) de beschrijving, als onderdeel van het jaarlijkse werkprogramma, en overeenkomstig de in punt f) van deze alinea bedoelde besluiten en met inachtneming van Verordeningen (EU) 2021/695 en (EU) 2021/694, van de in punt f) van deze alinea bedoelde gezamenlijke acties en de vaststelling van de voorwaarden voor de uitvoering van dergelijke gezamenlijke acties;
- h) de vaststelling van een procedure voor de benoeming van de uitvoerend directeur en de benoeming en het ontslag van de uitvoerend directeur, de verlenging van zijn ambtstermijn, en het geven van sturing aan en toezicht houden op de prestaties van de uitvoerend directeur;
- i) de vaststelling van richtsnoeren voor de beoordeling en de registratie van entiteiten als leden van de kennissamenleving;
- j) de vaststelling van de in artikel 10, lid 2, bedoelde werkafspraken;
- k) de benoeming van de rekenplichtige;
- l) de vaststelling van de jaarlijkse begroting van het kenniscentrum, met inbegrip van de overeenstemmende personeelsformatie waarin, uitgedrukt in voltijdequivalenten, het aantal tijdelijke betrekkingen per functiegroep en per rang, het aantal arbeidscontractanten en het aantal gedetacheerde nationale deskundigen is aangegeven;
- m) de vaststelling van transparantieregels voor het kenniscentrum en van regels voor het voorkomen en beheren van belangenconflicten, ook met betrekking tot de leden van de raad van bestuur, overeenkomstig artikel 42 van Ge-delegeerde Verordening (EU) 2019/715;
- n) de oprichting van werkgroepen binnen de kennissamenleving, in voorkomend geval rekening houdend met het advies van de strategische adviesgroep;
- o) de benoeming van leden van de strategische adviesgroep;
- p) de vaststelling van regels inzake de vergoeding van onkosten voor leden van de strategische adviesgroep;
- q) het opzetten van een controlemechanisme om ervoor te zorgen dat de uitvoering van de desbetreffende door het kenniscentrum beheerde fondsen gebeurt in overeenstemming met de agenda, de opdracht, het meerjarige werkprogramma en de regels van de programma's waaruit de relevante financiering wordt verstrekt;
- r) het zorgen voor regelmatig overleg en het vastleggen van een doeltreffend mechanisme voor samenwerking met de kennissamenleving;
- s) het opzetten van het communicatiebeleid van het kenniscentrum op basis van een aanbeveling van de uitvoerend directeur;
- t) in voorkomend geval, de vaststelling van regels ter uitvoering van het Statuut van de ambtenaren en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, vastgesteld bij Verordening (EEC, Euratom, ECSC) nr. 259/68 van de Raad ⁽¹⁵⁾ ("Statuut" en "Regeling"), overeenkomstig artikel 30, lid 3, van deze verordening;
- u) in voorkomend geval, de vaststelling van regels voor de detachering van nationale deskundigen bij het kenniscentrum en voor het inzetten van stagiairs overeenkomstig artikel 31, lid 2;
- v) de vaststelling van beveiligingsvoorschriften voor het kenniscentrum;
- w) de vaststelling van een strategie voor fraudebestrijding en corruptiebestrijding die in verhouding staat tot de fraude- en corruptierisico's, alsmede de vaststelling van uitgebreide maatregelen, overeenkomstig de toepasselijke wetgeving van de Unie, ter bescherming van personen die inbreuken op het Unierecht melden, rekening houdend met een kosten-batenanalyse van de uit te voeren maatregelen;
- x) indien nodig, de vaststelling van de methode voor de berekening van de vrijwillige financiële bijdrage en de bijdrage in natura van de bijdragende lidstaten overeenkomstig de Verordeningen (EU) 2021/695 en (EU) 2021/694 of andere toepasselijke wetgeving;

⁽¹⁵⁾ PB L 56 van 4.3.1968, blz. 1.

- y) het waarborgen, in de context van het jaarlijkse werkprogramma en het meerjarige werkprogramma, van samenhang en synergie met die delen van het programma Digitaal Europa en Horizon Europa die niet door het kenniscentrum worden beheerd, evenals met andere programma's van de Unie;
- z) de vaststelling van het jaarverslag over de uitvoering van de strategische doelstellingen en prioriteiten van het kenniscentrum, indien nodig met aanbevelingen met het oog op een betere verwezenlijking van deze doelstellingen en prioriteiten.

Voor zover het jaarlijkse werkprogramma gemeenschappelijke acties omvat, bevat het informatie over de vrijwillige bijdragen van de lidstaten aan gezamenlijke acties. In voorkomend geval wordt in de voorstellen, in het bijzonder in de voorstellen voor het jaarlijkse werkprogramma, beoordeeld of het nodig is de beveiligingsregels als bedoeld in artikel 33 van deze verordening toe te passen, met inbegrip van de procedure voor zelfbeoordeling inzake beveiliging overeenkomstig artikel 20 van Verordening (EU) 2021/695.

4. Wat de in lid 3, punten a), b) en c), beschreven besluiten betreft, houden de uitvoerend directeur en de raad van bestuur rekening met alle desbetreffende strategische adviezen en bijdragen van Enisa, overeenkomstig het door de raad van bestuur vastgestelde reglement van orde.

5. De raad van bestuur draagt de verantwoordelijkheid voor een adequate follow-up van de aanbevelingen in het in artikel 38, lid 2, bedoelde uitvoeringsverslag en in de in artikel 38, lid 4, bedoelde evaluatie.

Artikel 14

Voorzitter en vergaderingen van de raad van bestuur

1. De raad van bestuur kiest uit zijn leden een voorzitter en een vicevoorzitter voor een periode van drie jaar. De raad van bestuur kan besluiten het mandaat van de voorzitter en de vicevoorzitter eenmaal te verlengen. Indien het lidmaatschap van de raad van bestuur van de voorzitter of de vicevoorzitter echter tijdens hun ambtstermijn afloopt, loopt hun ambtstermijn automatisch op dat tijdstip af. De vicevoorzitter vervangt ambtshalve de voorzitter wanneer deze is verhinderd zijn taken te verrichten. De voorzitter neemt aan de stemming deel.
2. De raad van bestuur belegt ten minste driemaal per jaar een gewone vergadering. De raad van bestuur kan buitengewone vergaderingen beleggen op verzoek van de Commissie, op verzoek van een derde van al zijn leden, op verzoek van de voorzitter of op verzoek van de uitvoerend directeur met het oog op de vervulling van zijn taken.
3. De uitvoerend directeur neemt deel aan de beraadslagingen van de raad van bestuur tenzij de raad van bestuur daar anders over beslist, maar heeft geen stemrecht.
4. De raad van bestuur kan per geval andere personen uitnodigen om de vergaderingen als waarnemer bij te wonen.
5. De voorzitter kan vertegenwoordigers van de kennissamenleving uitnodigen om deel te nemen aan de vergaderingen van de raad van bestuur, maar zij hebben geen stemrecht.
6. De leden van de raad van bestuur en hun plaatsvervangers kunnen zich, onder voorbehoud van de bepalingen van het reglement van orde, tijdens de vergaderingen laten bijstaan door adviseurs of deskundigen.
7. Het kenniscentrum vervult de secretariaatstaken voor de raad van bestuur.

Artikel 15

Stemregels in de raad van bestuur

1. Bij zijn besprekingen streeft de raad van bestuur consensus na. Er wordt een stemming gehouden indien de leden van de raad van bestuur geen consensus hebben bereikt.
2. Indien de raad van bestuur geen consensus over een aangelegenheid bereikt, neemt hij zijn besluiten met een meerderheid van ten minste 75 % van de stemmen van al zijn leden, waarbij de vertegenwoordigers van de Commissie voor dit doel één enkel lid vormen. Een afwezig lid van de raad van bestuur kan zijn stemrecht overdragen aan zijn plaatsvervanger of, in afwezigheid van zijn plaatsvervanger, aan een ander lid. Een lid van de raad van bestuur mag niet meer dan één ander lid vertegenwoordigen.

3. De in de punten f) en g) van artikel 13, lid 3, genoemde besluiten van de raad van bestuur betreffende de gezamenlijke acties en het beheer ervan worden als volgt vastgesteld:
 - a) besluiten om middelen uit de begroting van de Unie toe te wijzen aan gezamenlijke acties als bedoeld in artikel 13, lid 3, punt f), en besluiten tot het opnemen van dergelijke gezamenlijke acties in het jaarlijkse werkprogramma, worden genomen overeenkomstig lid 2 van dit artikel;
 - b) besluiten met betrekking tot de beschrijving van gezamenlijke acties en de vaststelling van de voorwaarden voor de uitvoering ervan als bedoeld in artikel 13, lid 3, punt g), worden genomen door de deelnemende lidstaten en de Commissie, waarbij het stemrecht van de leden in verhouding dient te staan tot hun respectieve bijdragen aan die gezamenlijke actie, berekend overeenkomstig de krachtens artikel 13, lid 3, punt x), vastgestelde methode.
4. Voor besluiten die worden genomen op grond van artikel 13, lid 3, punten b), c), d), e), f), k), l), p), q), t), u), w), x) en y), heeft de Commissie 26 % van het totale aantal stemmen in de raad van bestuur.
5. Voor andere besluiten dan die bedoeld in lid 3, punt b), en lid 4 krijgt elke lidstaat alsook de Unie één stem. De stem van de Unie wordt door de twee vertegenwoordigers van de Commissie gezamenlijk uitgebracht.
6. De voorzitter neemt deel aan de stemming.

Afdeling II

Uitvoerend directeur

Artikel 16

Benoeming, ontslag en verlenging van de ambtstermijn van de uitvoerend directeur

1. De uitvoerend directeur beschikt over deskundigheid en heeft een sterke reputatie op de gebieden waarop het kenniscentrum opereert.
2. De uitvoerend directeur wordt in dienst genomen als een tijdelijke functionaris van het kenniscentrum overeenkomstig artikel 2, punt a), van de Regeling.
3. De uitvoerend directeur wordt na een open, transparante en niet-discriminerende selectieprocedure door de raad van bestuur aangesteld uit een lijst van door de Commissie voorgedragen kandidaten.
4. Voor de sluiting van het contract met de uitvoerend directeur wordt het kenniscentrum vertegenwoordigd door de voorzitter van de raad van bestuur.
5. De ambtstermijn van de uitvoerend directeur bedraagt vier jaar. Vóór het eind van deze termijn voert de Commissie een beoordeling uit waarin rekening wordt gehouden met de evaluatie van de prestaties van de uitvoerend directeur en de toekomstige taken en opgaven van het kenniscentrum.
6. Op voorstel van de Commissie, die rekening houdt met de in lid 5 bedoelde beoordeling, kan de raad van bestuur de ambtstermijn van de uitvoerend directeur eenmaal verlengen met ten hoogste vier jaar.
7. Een uitvoerend directeur wiens ambtstermijn is verlengd, mag niet deelnemen aan een andere selectieprocedure voor dezelfde betrekking.
8. De uitvoerend directeur wordt uitsluitend uit zijn functie ontheven bij besluit van de raad van bestuur op voorstel van de Commissie of van ten minste 50 % van de lidstaten.

Artikel 17

Taken van de uitvoerend directeur

1. De uitvoerend directeur is verantwoordelijk voor de werkzaamheden en de dagelijkse leiding en is de wettelijke vertegenwoordiger van het kenniscentrum. De uitvoerend directeur legt verantwoording af aan de raad van bestuur en verricht zijn taken in alle onafhankelijkheid binnen de grenzen van de hem verleende bevoegdheden. De uitvoerend directeur wordt ondersteund door het personeel van het kenniscentrum.
2. De uitvoerend directeur voert op onafhankelijke wijze ten minste de volgende taken uit:
 - a) de besluiten van de raad van bestuur uitvoeren;
 - b) de werkzaamheden van de raad van bestuur ondersteunen, het secretariaat van zijn vergaderingen verzorgen en alle informatie verstrekken die voor de uitvoering van zijn taken nodig is;

- c) na overleg met de raad van bestuur en de Commissie en rekening houdend met de bijdragen van de nationale coördinatiecentra en de kennisgemeenschap, de agenda alsook, in overeenstemming met de agenda, het ontwerp van het jaarlijkse werkprogramma en het ontwerp van het meerjarige werkprogramma van het kenniscentrum opstellen en ter goedkeuring aan de raad van bestuur voorleggen, met inbegrip van de reikwijdte van de oproepen tot het indienen van voorstellen, van de oproepen tot het indienen van blijken van belangstelling en van de aanbestedingen die nodig zijn voor de uitvoering van het jaarlijkse werkprogramma, en de bijbehorende uitgavenramingen, zoals voorgesteld door de lidstaten en de Commissie;
- d) het ontwerp van de jaarbegroting opstellen en ter goedkeuring aan de raad van bestuur voorleggen; dit omvat ook de in artikel 13, lid 3, punt l), bedoelde bijbehorende personeelsformatie waarin, uitgedrukt in voltijdequivalenten, het aantal tijdelijke betrekkingen per rang en per functiegroep, het aantal arbeidscontractanten en het aantal gedetacheerde nationale deskundigen wordt vermeld;
- e) het jaarlijkse werkprogramma en het meerjarige werkprogramma uitvoeren en daarover verslag uitbrengen aan de raad van bestuur;
- f) het ontwerp van jaarlijks activiteitenverslag van het kenniscentrum opstellen, met daarin de informatie over de overeenkomstige uitgaven en de verwezenlijking van de agenda en het meerjarige werkprogramma; indien nodig gaat dat verslag vergezeld van voorstellen voor verdere verbeteringen bij de verwezenlijking of de herformulering van de strategische doelstellingen en prioriteiten;
- g) zorgen voor de uitvoering van doeltreffende toezichts- en evaluatieprocedures met betrekking tot de prestaties van het kenniscentrum;
- h) een actieplan opstellen waarmee uitvoering wordt gegeven aan de conclusies van het in artikel 38, lid 2, bedoelde uitvoeringsverslag en de in artikel 38, lid 4, bedoelde evaluatie, en om de twee jaar een verslag indienen over de geboekte vooruitgang bij het Europees Parlement en de Commissie;
- i) overeenkomsten met de nationale coördinatiecentra opstellen en sluiten;
- j) de verantwoordelijkheid dragen voor administratieve, financiële en personeelsaangelegenheden, met inbegrip van de uitvoering van de begroting van het kenniscentrum, waarbij terdege rekening wordt gehouden met het advies van de relevante interneauditfunctie, binnen de grenzen van de in artikel 13, lid 3, punten e), l), t), u), v) en w), bedoelde besluiten;
- k) de uitschrijving van oproepen tot het indienen van voorstellen goedkeuren en beheren in overeenstemming met het jaarlijkse werkprogramma, en de daaruit resulterende subsidieovereenkomsten en -besluiten beheren;
- l) de lijst goedkeuren van acties die voor financiering zijn geselecteerd op basis van een door een panel van onafhankelijke deskundigen opgestelde ranglijst;
- m) de uitschrijving van aanbestedingen goedkeuren en beheren in overeenstemming met het jaarlijkse werkprogramma, en de daaruit resulterende contracten beheren;
- n) de voor financiering geselecteerde offertes goedkeuren;
- o) het ontwerp van jaarrekening en jaarbalans voorleggen aan de relevante interneauditfunctie, en vervolgens aan de raad van bestuur;
- p) zorgen voor risicoanalyses en risicobeheer;
- q) afzonderlijke subsidieovereenkomsten, -besluiten en -contracten ondertekenen;
- r) contracten voor opdrachten ondertekenen;
- s) een actieplan opstellen waarmee uitvoering wordt gegeven aan de conclusies van interne of externe auditverslagen, alsook van onderzoeken van het Europees Bureau voor fraudebestrijding (OLAF), opgericht bij Besluit 1999/352/EG, EGKS, Euratom van de Commissie ⁽¹⁶⁾ en tweemaal per jaar aan de Commissie en op regelmatige tijdstippen aan de raad van bestuur verslag uitbrengen over de geboekte vooruitgang;
- t) een ontwerp van financiële regeling opstellen die van toepassing is op het kenniscentrum;
- u) een doeltreffend en doelmatig internecontrolesysteem instellen, toezien op de werking ervan en elke ingrijpende wijziging daarin aan de raad van bestuur melden;

⁽¹⁶⁾ Besluit 1999/352/EG, EGKS, Euratom van de Commissie van 28 april 1999 houdende oprichting van het Europees Bureau voor fraudebestrijding (OLAF) (PB L 136 van 31.5.1999, blz. 20).

- v) zorgen voor doeltreffende communicatie met de instellingen van de Unie en op verzoek verslag uitbrengen aan het Europees Parlement en de Raad;
- w) alle andere maatregelen nemen die nodig zijn voor de beoordeling of het kenniscentrum succes boekt bij de verwezenlijking van zijn opdracht en doelstellingen;
- x) alle andere taken uitvoeren die de raad van bestuur aan hem heeft toevertrouwd of gedelegeerd.

Afdeling III

Strategische adviesgroep

Artikel 18

Samenstelling van de strategische adviesgroep

1. De strategische adviesgroep bestaat uit maximaal twintig leden. De leden worden op voordracht van de uitvoerend directeur door de raad van bestuur benoemd uit de vertegenwoordigers van de leden van de kennissamenleving die geen vertegenwoordigers van instellingen, organen of instanties van de Unie zijn. Alleen vertegenwoordigers van leden die niet onder de zeggenschap vallen van een derde land of een in een derde land gevestigde entiteit, komen in aanmerking. De benoeming geschiedt volgens een open, transparante en niet-discriminerende procedure. De raad van bestuur streeft ernaar de strategische adviesgroep zo samen te stellen dat de kennissamenleving evenwichtig vertegenwoordigd is, waarbij er niet alleen een evenwicht is tussen wetenschappelijke, industriële en maatschappelijke entiteiten, bedrijfstakken aan de vraag- en aanbodzijde, grote ondernemingen en kmo's, maar ook qua geografische herkomst en geslacht. Hij streeft ook naar een evenwichtige samenstelling tussen sectoren, rekening houdend met de cohesie van de Unie en alle lidstaten op het gebied van onderzoek, industrie en technologie op het gebied van cyberbeveiliging. De strategische adviesgroep wordt zo samengesteld dat er een integrale, continue en permanente dialoog tussen de kennissamenleving en het kenniscentrum mogelijk is.
2. De leden van de strategische adviesgroep beschikken over deskundigheid met betrekking tot onderzoek op het gebied van cyberbeveiliging, industriële ontwikkeling en het aanbieden, uitvoeren of inzetten van professionele diensten of producten. De vereisten met betrekking tot dergelijke deskundigheid worden nader gespecificeerd door de raad van bestuur.
3. De procedures voor de benoeming van de leden van de strategische adviesgroep en de werking van de strategische adviesgroep worden vastgelegd in het reglement van orde van de raad van bestuur en worden openbaar gemaakt.
4. De ambtstermijn van de leden van de strategische adviesgroep bedraagt twee jaar. Deze termijn kan eenmaal worden verlengd.
5. Vertegenwoordigers van de Commissie en van andere instellingen, organen en instanties van de Unie, met name Enisa, kunnen door de strategische adviesgroep worden uitgenodigd om deel te nemen aan haar werkzaamheden en die te ondersteunen. De strategische adviesgroep kan per geval extra vertegenwoordigers van de kennissamenleving uitnodigen als waarnemer, adviseur of deskundige, al naargelang, om rekening te houden met de dynamiek van ontwikkelingen op het gebied van cyberbeveiliging. De leden van de raad van bestuur kunnen als waarnemer deelnemen aan de vergaderingen van de strategische adviesgroep.

Artikel 19

Werking van de strategische adviesgroep

1. De strategische adviesgroep komt ten minste driemaal per jaar bijeen.
2. De strategische adviesgroep geeft de raad van bestuur advies over de oprichting van werkgroepen binnen de kennissamenleving overeenkomstig artikel 13, lid 3, punt n), in verband met specifieke kwesties die van belang zijn voor de werkzaamheden van het kenniscentrum, wanneer deze kwesties direct verband houden met de in artikel 20 genoemde taken en bevoegdheden. Indien nodig vallen dergelijke werkgroepen onder de algemene coördinatie van een of meer leden van de strategische adviesgroep.
3. De strategische adviesgroep kiest haar voorzitter bij gewone meerderheid van de leden.
4. Het secretariaat van de strategische adviesgroep wordt verzorgd door de uitvoerend directeur en het personeel van het kenniscentrum, met gebruikmaking van de bestaande middelen, met inachtneming van de totale werklast van het kenniscentrum. De middelen bestemd voor de ondersteuning van de strategische adviesgroep worden vermeld in de ontwerpbegroting.
5. De strategische adviesgroep neemt zijn reglement van orde aan bij gewone meerderheid van haar leden.

*Artikel 20***Taken van de strategische adviesgroep**

De strategische adviesgroep adviseert het kenniscentrum regelmatig over de uitvoering van de activiteiten van het kenniscentrum en zorgt voor communicatie met de kennissamenleving en andere betrokken belanghebbenden. De strategische adviesgroep doet ook het volgende:

- a) zij verstrekt, rekening houdend met bijdragen van de kennissamenleving en, in voorkomend geval, van de in artikel 13, lid 3, punt n), bedoelde werkgroepen, binnen de door de raad van bestuur vastgestelde termijnen, de uitvoerend directeur en de raad van bestuur strategisch advies en input met betrekking tot de agenda en de jaarlijkse en meerjarige werkprogramma's, en werkt dit voortdurend bij;
- b) zij adviseert de raad van bestuur over het instellen van werkgroepen binnen de kennissamenleving overeenkomstig artikel 13, lid 3, punt n), over specifieke kwesties die van belang zijn voor de werkzaamheden van het kenniscentrum;
- c) zij neemt, na goedkeuring door de raad van bestuur, een besluit over en organiseert openbare raadplegingen waaraan alle publieke en private stakeholders die een belang hebben op het gebied van cyberbeveiliging kunnen deelnemen, teneinde de input voor het in punt a) bedoelde strategische advies te verzamelen.

*HOOFDSTUK III***Financiële bepalingen***Artikel 21***Financiële bijdrage van de Unie en de lidstaten**

1. Het kenniscentrum wordt gefinancierd door de Unie en gezamenlijke acties worden gefinancierd door de Unie en met vrijwillige bijdragen van de lidstaten.
2. De administratieve en operationele kosten van gezamenlijke acties worden gedragen door de Unie en de lidstaten die bijdragen aan de gezamenlijke acties, in overeenstemming met de verordeningen (EU) 2021/695 en (EU) 2021/694.
3. De bijdrage van de Unie voor de administratieve en operationele kosten van het kenniscentrum omvat:
 - a) tot 1 649 566 000 EUR uit het programma Digitaal Europa, waaronder tot maximaal 32 000 000 EUR voor administratieve kosten;
 - b) een bedrag uit Horizon Europa, onder meer voor administratieve kosten, voor gezamenlijke acties, waarbij dat bedrag gelijk is aan het bedrag dat de lidstaten overeenkomstig lid 7 van dit artikel hebben bijgedragen, maar niet groter is dan het bedrag dat is vastgelegd in het strategische planningsproces van Horizon Europa dat moet worden uitgevoerd overeenkomstig artikel 6, lid 6, van Verordening (EU) 2021/695, in het jaarlijkse werkprogramma of in het meerjarige werkprogramma;
 - c) een bedrag uit de andere desbetreffende programma's van de Unie dat nodig is voor de uitvoering van de taken of de verwezenlijking van de doelstellingen van het kenniscentrum, onder voorbehoud van besluiten die worden genomen overeenkomstig de rechtshandelingen van de Unie tot vaststelling van die programma's.
4. De maximale bijdrage van de Unie wordt betaald uit de kredieten van de algemene begroting van de Unie die zijn toegewezen aan het programma Digitaal Europa, het specifieke programma tot uitvoering van Horizon Europa vastgesteld bij Besluit (EU) 2021/764 en andere programma's en projecten die tot het activiteitengebied van het kenniscentrum of het netwerk behoren.
5. Het kenniscentrum voert overeenkomstig artikel 62, lid 1, eerste alinea, punt c), iv), van het Financieel Reglement maatregelen uit van het programma Digitaal Europa en Horizon Europa op het gebied van cyberbeveiliging.
6. Bijdragen uit andere dan de in de leden 3 en 4 bedoelde programma's van de Unie die onderdeel zijn van de medefinanciering door de Unie van een programma dat door een van de lidstaten wordt uitgevoerd, worden niet in aanmerking genomen voor de berekening van de in die leden bedoelde maximale financiële bijdrage van de Unie.
7. De lidstaten nemen vrijwillig deel aan gezamenlijke acties door middel van vrijwillige financiële bijdragen en/of bijdragen in natura. Indien een lidstaat deelneemt aan een gezamenlijke actie, dekt de financiële bijdrage van die lidstaat de administratieve kosten in verhouding tot zijn bijdrage aan die gezamenlijke actie. De administratieve kosten van gezamenlijke acties worden betaald met financiële bijdragen. De operationele kosten van gezamenlijke acties kunnen worden betaald met financiële bijdragen of bijdragen in natura, zoals bepaald in Horizon Europa en het programma Digitaal Europa. De bijdragen van een lidstaat kunnen de vorm aannemen van steun die de lidstaat levert in het kader van een gezamenlijke actie aan in die lidstaat gevestigde begunstigen. Bijdragen in natura van de lidstaten worden gevormd door de subsidiabele kosten die worden gemaakt door de nationale coördinatiecentra en andere publieke entiteiten wanneer zij deelnemen aan projecten die uit hoofde van deze verordening worden gefinancierd, verminderd met een

eventuele bijdrage van de Unie aan die kosten. Voor projecten die uit Horizon Europa worden gefinancierd, worden de subsidiabele kosten berekend overeenkomstig artikel 36 van Verordening (EU) 2021/695. Voor projecten die uit het programma Digitaal Europa worden gefinancierd, worden de subsidiabele kosten berekend overeenkomstig het Financieel Reglement.

Het beoogde bedrag van de totale vrijwillige bijdragen van de lidstaten aan gezamenlijke acties in het kader van Horizon Europa, onder meer financiële bijdragen voor administratieve kosten, wordt vastgelegd teneinde in aanmerking te worden genomen in het strategische planningsproces van Horizon Europa dat overeenkomstig artikel 6, lid 6, van Verordening (EU) 2021/695 moet worden uitgevoerd, met inbreng van de raad van bestuur. Voor acties in het kader van het programma Digitaal Europa kunnen de lidstaten, niettegenstaande artikel 15 van Verordening (EU) 2021/694, een bijdrage leveren aan de kosten van het kenniscentrum die worden medegefinancierd uit het programma Digitaal Europa die lager is dan de in lid 3, punt a), van dit artikel vermelde bedragen.

8. De nationale medefinanciering door de lidstaten van acties die door andere programma's van de Unie dan Horizon Europa en het programma Digitaal Europa worden ondersteund, wordt beschouwd als nationale bijdragen van de lidstaten voor zover deze bijdragen deel uitmaken van gezamenlijke acties en zijn opgenomen in het werkprogramma van het kenniscentrum.

9. Voor de beoordeling van de in lid 3 van dit artikel en in artikel 22, lid 2, punt b), bedoelde bijdragen worden kosten vastgesteld overeenkomstig de gebruikelijke kostenberekeningsmethoden van de desbetreffende lidstaten, overeenkomstig de in die lidstaat toepasselijke boekhoudkundige normen en overeenkomstig de toepasselijke internationale boekhoudkundige normen en internationale normen voor financiële verslaglegging. Kosten worden gecertificeerd door een onafhankelijke externe auditor die is aangewezen door de betrokken lidstaat. De waarderingsmethode van de bijdragen kan door het kenniscentrum worden geverifieerd indien er onduidelijkheid is ontstaan door de certificering.

10. Indien een lidstaat zijn verplichtingen in verband met zijn financiële bijdrage of bijdrage in natura aan gezamenlijke acties niet nakomt, maakt de uitvoerend directeur daarvan schriftelijk melding aan de betrokken lidstaat en stelt hij een redelijke termijn vast waarbinnen die niet-nakoming dient te worden verholpen. Indien dit niet binnen die termijn is gebeurd, roept de uitvoerend directeur een vergadering van de raad van bestuur bijeen om te besluiten of het stemrecht van de in gebreke blijvende deelnemende lidstaat moet worden ingetrokken, dan wel of andere maatregelen moeten worden genomen totdat die lidstaat zijn verbintenissen is nagekomen. Het stemrecht betreffende gezamenlijke acties van de in gebreke blijvende lidstaat wordt opgeschort totdat hij zijn verplichtingen nakomt.

11. De Commissie kan de financiële bijdrage van de Unie aan gezamenlijke acties beëindigen, proportioneel verlagen of schorsen, indien de bijdragende lidstaten de in lid 3, punt b), bedoelde bijdragen niet, slechts gedeeltelijk of te laat verstrekken. De beëindiging, verlaging of schorsing door de Commissie van de financiële bijdrage van de Unie is qua bedrag en duur proportioneel met de niet-verstrekking, de slechts gedeeltelijke verstrekking of de te late verstrekking van de bijdragen door de lidstaat.

12. De bijdragende lidstaten brengen jaarlijks uiterlijk op 31 januari aan de raad van bestuur verslag uit over de hoogte van de bijdragen die zij in het voorgaande begrotingsjaar overeenkomstig lid 7 voor gezamenlijke acties met de Unie hebben gedaan.

Artikel 22

Kosten en middelen van het kenniscentrum

1. De administratieve kosten van het kenniscentrum worden in beginsel gefinancierd uit financiële bijdragen op jaarbasis van de Unie. Extra financiële bijdragen worden geleverd door bijdragende lidstaten in verhouding tot hun vrijwillige bijdrage aan gezamenlijke acties. Indien een deel van de bijdragen voor de administratieve kosten niet wordt gebruikt, kan het ter beschikking worden gesteld om de operationele kosten van het kenniscentrum te dekken.

2. De operationele kosten van het kenniscentrum worden gedekt door:

- a) de financiële bijdrage van de Unie;
- b) vrijwillige financiële bijdragen of bijdragen in natura van de bijdragende lidstaten, bij gezamenlijke acties.

3. De in de begroting van het kenniscentrum opgenomen middelen bestaan uit de volgende bijdragen:

- a) de financiële bijdragen van de Unie aan de operationele en administratieve kosten;
- b) vrijwillige financiële bijdragen van de bijdragende lidstaten voor de administratieve kosten bij gezamenlijke acties;
- c) vrijwillige financiële bijdragen van de bijdragende lidstaten voor de operationele kosten bij gezamenlijke acties;

- d) alle inkomsten die door het kenniscentrum worden gegenereerd;
- e) alle andere financiële bijdragen, middelen of inkomsten.
4. Intresten op de bijdragen die door de bijdragende lidstaten aan het kenniscentrum worden betaald, gelden als inkomsten van het kenniscentrum.
5. Alle middelen van het kenniscentrum en zijn activiteiten worden aangewend om zijn doelstellingen te bereiken.
6. Het kenniscentrum is eigenaar van alle activa die het genereert of die eraan zijn overgedragen voor de verwezenlijking van zijn doelstellingen. Onverminderd de toepasselijke regels van het desbetreffende financieringsprogramma wordt de eigendom van activa die zijn gegenereerd of verworven in het kader van gezamenlijke acties, vastgesteld overeenkomstig artikel 15, lid 3, punt b).
7. Behalve bij ontbinding van het kenniscentrum blijven de inkomsten, voor zover zij meer bedragen dan de uitgaven, in handen van het kenniscentrum en worden zij niet aan de bijdragende leden van het kenniscentrum uitbetaald.
8. Het kenniscentrum werkt nauw samen met andere instellingen, organen en instanties van de Unie, met inachtneming van hun respectieve mandaten en zonder overlapping met bestaande samenwerkingsmechanismen, teneinde synergie met hen te benutten en, waar mogelijk en dienstig, de administratieve kosten te verminderen.

Artikel 23

Financieringsinstrumenten

De financiële verbintenissen van het kenniscentrum mogen het bedrag van de beschikbare of door zijn leden voor zijn begroting vastgelegde financiële middelen niet overschrijden.

Artikel 24

Financieringsinstrumenten

Het begrotingsjaar begint op 1 januari en eindigt op 31 december.

Artikel 25

Vaststelling van de begroting

1. De uitvoerend directeur stelt jaarlijks een ontwerpraming op van de ontvangsten en uitgaven van het kenniscentrum voor het volgende begrotingsjaar en zendt die, samen met het in artikel 13, lid 3, punt l), bedoelde ontwerpoverzicht van de personeelsformatie, aan de raad van bestuur. De ontvangsten en uitgaven moeten in evenwicht zijn. De uitgaven van het kenniscentrum omvatten de personele, administratieve, infrastructurele en operationele uitgaven. De administratieve uitgaven worden tot een minimum beperkt, onder meer door herschikking van personeel of betrekkingen.
2. De raad van bestuur stelt jaarlijks de raming van de ontvangsten en uitgaven van het kenniscentrum voor het volgende begrotingsjaar vast op basis van de in lid 1 bedoelde ontwerpraming van de ontvangsten en uitgaven.
3. Uiterlijk 31 januari van elk jaar stuurt de raad van bestuur de in lid 2 van dit artikel bedoelde raming, die deel uitmaakt van het ontwerp van enig programmeringsdocument bedoeld in artikel 32, lid 1, van Gedelegeerde Verordening (EU) 2019/715, naar de Commissie.
4. Op basis van de raming bedoeld in lid 2 van dit artikel, neemt de Commissie in het ontwerp van algemene begroting van de Unie de ramingen op die zij nodig acht voor de personeelsformatie bedoeld in artikel 13, lid 3, punt l), van deze verordening alsook het bedrag van de bijdrage ten laste van de algemene begroting, die zij overeenkomstig de artikelen 313 en 314 van het Verdrag betreffende de werking van de Europese Unie (VWEU) bij het Europees Parlement en de Raad indient.
5. Het Europees Parlement en de Raad keuren de kredieten voor de bijdrage aan het kenniscentrum goed.
6. Het Europees Parlement en de Raad stellen de in artikel 13, lid 3, punt l), bedoelde personeelsformatie vast.

7. De raad van bestuur stelt samen met het jaarlijkse werkprogramma en het meerjarige werkprogramma de begroting van het kenniscentrum vast. De begroting wordt definitief na de definitieve vaststelling van de algemene begroting van de Unie. Indien nodig past de raad van bestuur de begroting en het jaarlijkse werkprogramma van het kenniscentrum aan in overeenstemming met de algemene begroting van de Unie.

Artikel 26

Indiening van de rekeningen van het kenniscentrum en kwijting

De indiening van de voorlopige en de definitieve rekeningen van het kenniscentrum en de kwijting verlopen volgens de regels en het tijdschema van het Financieel Reglement en van de financiële regels van het kenniscentrum.

Artikel 27

Operationele en financiële verslaglegging

1. De uitvoerend directeur brengt jaarlijks verslag uit aan de raad van bestuur over de uitvoering van zijn taken in overeenstemming met de financiële regels van het kenniscentrum.

2. Binnen twee maanden na het einde van het begrotingsjaar legt de uitvoerend directeur de raad van bestuur ter goedkeuring een jaarlijks activiteitenverslag voor over de door het kenniscentrum in het voorafgaande kalenderjaar gemaakte vorderingen, met name ten aanzien van het jaarlijkse werkprogramma voor dat jaar, en de verwezenlijking van zijn strategische doelstellingen en prioriteiten. Dit verslag bevat onder meer informatie over het volgende:

- a) uitgevoerde operationele acties en de daarmee verband houdende uitgaven;
 - b) de ingediende acties, met inbegrip van een opsplitsing per soort deelnemer, waaronder kleine en middelgrote ondernemingen, en per lidstaat;
 - c) de voor financiering aangewezen acties, met inbegrip van een opsplitsing per soort deelnemer, waaronder kmo's, en per lidstaat, met vermelding van de bijdrage van het kenniscentrum aan de afzonderlijke deelnemers en acties;
 - d) de verwezenlijking van de in deze verordening vastgestelde opdracht en doelstellingen, en voorstellen voor verdere noodzakelijke werkzaamheden ter verwezenlijking van die opdracht en die doelstellingen;
 - e) de samenhang van de uitvoeringstaken met de agenda en het meerjarige werkprogramma.
3. Na goedkeuring door de raad van bestuur wordt het jaarlijkse activiteitenverslag openbaar gemaakt.

Artikel 28

Financiële regels

Het kenniscentrum stelt zijn specifieke financiële regels vast overeenkomstig artikel 70 van het Financieel Reglement.

Artikel 29

Bescherming van de financiële belangen van de Unie

1. Het kenniscentrum neemt de nodige maatregelen om ervoor te zorgen dat bij de uitvoering van uit hoofde van deze verordening gefinancierde acties, de financiële belangen van de Unie worden beschermd met preventieve maatregelen tegen fraude, corruptie en andere onwettige activiteiten, met regelmatige en doeltreffende controles en, indien onregelmatigheden worden ontdekt, terugvordering van de onterecht betaalde bedragen en, voor zover van toepassing, met doeltreffende, evenredige en afschrikkende bestuurlijke sancties.

2. Het kenniscentrum verleent personeelsleden van de Commissie en andere door haar gemachtigde personen alsmede de Rekenkamer toegang tot de terreinen en gebouwen van het kenniscentrum en tot alle informatie, ook in elektronisch formaat, die benodigd is voor het verrichten van hun controles.

3. OLAF kan overeenkomstig de bepalingen en procedures van Verordening (Euratom, EG) nr. 2185/96 van de Raad⁽¹⁷⁾ en Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad⁽¹⁸⁾ onderzoeken instellen, met inbegrip van controles en verificaties ter plaatse, om vast te stellen of er sprake is geweest van fraude, corruptie of andere onwettige activiteiten in verband met een subsidieovereenkomst of een direct of indirect uit hoofde van deze verordening gefinancierd contract, waardoor de financiële belangen van de Unie zijn geschaad.

4. Onverminderd de leden 1, 2 en 3 bevatten de contracten en subsidieovereenkomsten die uit de toepassing van deze verordening voortvloeien, bepalingen die de Commissie, het kenniscentrum, de Rekenkamer en OLAF uitdrukkelijk de bevoegdheid geven dergelijke controles en onderzoeken binnen hun respectieve bevoegdheden te verrichten. Indien de uitvoering van een actie geheel of gedeeltelijk uitbesteed of verder gedelegeerd wordt, of indien hiervoor een overheidsopdracht moet worden geplaatst of financiële steun moet worden verleend aan een derde, wordt in het contract of de subsidieovereenkomst bepaald dat de contractant of de begunstigde ervan verplicht is van elke betrokken derde te verlangen dat deze uitdrukkelijk de bevoegdheid van de Commissie, het kenniscentrum, de Rekenkamer en OLAF aanvaardt.

HOOFDSTUK IV

Personeel van het kenniscentrum

Artikel 30

Personeel

1. Het Statuut en de Regeling en de door de instellingen van de Unie gezamenlijk vastgestelde regelingen ter uitvoering van het Statuut en de Regeling, zijn van toepassing op het personeel van het kenniscentrum.

2. De raad van bestuur oefent met betrekking tot het personeel van het kenniscentrum de bevoegdheden uit die krachtens het Statuut aan het tot aanstelling bevoegde gezag zijn toegekend en de bevoegdheden die krachtens de Regeling die van toepassing is op de andere personeelsleden zijn toegekend aan het tot het sluiten van arbeidscontracten bevoegde gezag (de "bevoegdheden tot aanstelling").

3. Overeenkomstig artikel 110 van het Statuut stelt de raad van bestuur, op grond van artikel 2, lid 1, van het Statuut en van artikel 6 van de Regeling die van toepassing is op de andere personeelsleden, een besluit vast om de bevoegdheden tot aanstelling te delegeren aan de uitvoerend directeur en de voorwaarden vast te stellen waaronder die delegatie kan worden geschorst. De uitvoerend directeur mag deze bevoegdheid subdelegeren.

4. Indien uitzonderlijke omstandigheden dit vereisen, kan de raad van bestuur een besluit nemen om de delegatie van de bevoegdheden tot aanstelling aan de uitvoerend directeur en elke door deze laatste verleende subdelegatie te schorsen. De raad van bestuur oefent in een dergelijk geval de bevoegdheden tot aanstelling zelf uit of delegeert deze aan een van zijn leden of aan een ander personeelslid van het kenniscentrum dan de uitvoerend directeur.

5. De raad van bestuur stelt overeenkomstig artikel 110 van het Statuut bepalingen vast voor de tenuitvoerlegging van het Statuut en de Regeling.

6. De personele middelen worden vastgelegd in de in artikel 13, lid 3, punt l), bedoelde personeelsformatie waarin, uitgedrukt in voltijdequivalenten en in overeenstemming met de jaarbegroting van het kenniscentrum, het aantal tijdelijke betrekkingen per functiegroep en per rang evenals het aantal arbeidscontractanten worden vermeld.

7. In de benodigde personele middelen van het kenniscentrum wordt in eerste instantie voorzien door herschikking van personeel of betrekkingen van de instellingen, organen en instanties van de Unie, alsook door de aanwerving van extra personeel. Het personeel van het kenniscentrum kan bestaan uit tijdelijke functionarissen en arbeidscontractanten.

⁽¹⁷⁾ Verordening (Euratom, EG) nr. 2185/96 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Europese Gemeenschappen tegen fraudes en andere onregelmatigheden (PB L 292 van 15.11.1996, blz. 2).

⁽¹⁸⁾ Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11 september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) en tot intrekking van Verordening (EG) nr. 1073/1999 van het Europees Parlement en de Raad en Verordening (Euratom) nr. 1074/1999 van de Raad (PB L 248 van 18.9.2013, blz. 1).

8. Alle personeelskosten zijn ten laste van het kenniscentrum.

Artikel 31

Gedetacheerde nationale deskundigen en andere personeelsleden

1. Het kenniscentrum kan gebruikmaken van gedetacheerde nationale deskundigen of ander personeel dat niet in dienst is van het kenniscentrum.
2. In overleg met de Commissie stelt de raad van bestuur een besluit vast met regels voor de detachering van nationale deskundigen bij het kenniscentrum.

Artikel 32

Voorrechten en immuniteiten

Protocol nr. 7 inzake voorrechten en immuniteiten van de Europese Unie, dat aan het VEU en aan het VWEU is gehecht, is van toepassing op het kenniscentrum en zijn personeelsleden.

HOOFDSTUK V

Gemeenschappelijke bepalingen

Artikel 33

Veiligheidsregels

1. Artikel 12 van Verordening (EU) 2021/694 is van toepassing op de deelname aan alle door het kenniscentrum gefinancierde acties.
2. Voor uit Horizon Europa gefinancierde acties gelden de volgende specifieke veiligheidsvoorschriften:
 - a) voor de toepassing van artikel 38, lid 1, van Verordening (EU) 2021/695 kan, indien het jaarlijkse werkprogramma hierin voorziet, de verlening van niet-exclusieve licenties worden beperkt tot derden die zijn gevestigd of geacht worden te zijn gevestigd in een lidstaat en waarover die lidstaat of onderdanen van die lidstaat zeggenschap uitoefenen;
 - b) voor de toepassing van artikel 40, lid 4, eerste alinea, punt b), van Verordening (EU) 2021/695 is de overdracht of licentieverlening aan een in een geassocieerd land gevestigde juridische entiteit of aan een in de Unie gevestigde juridische entiteit waarover vanuit derde landen zeggenschap wordt uitgeoefend, een grond voor bezwaar tegen de overdracht van de eigendom van resultaten of tegen de verlening van een exclusieve licentie voor resultaten;
 - c) voor de toepassing van artikel 41, lid 7, eerste alinea, punt a), van Verordening (EU) 2021/695 kan, indien het jaarlijkse werkprogramma hierin voorziet, de verlening van in artikel 2, punt 9, van die verordening bedoelde toegangsrechten worden beperkt tot uitsluitend juridische entiteiten die zijn gevestigd of geacht worden te zijn gevestigd in een lidstaat en waarover die lidstaat of onderdanen van die lidstaat zeggenschap uitoefenen.

Artikel 34

Transparantie

1. Het kenniscentrum verricht zijn werkzaamheden met een hoge mate van transparantie.
2. Het kenniscentrum ziet erop toe dat het publiek en alle belanghebbenden tijdig van passende, objectieve, betrouwbare en gemakkelijk toegankelijke informatie worden voorzien, in het bijzonder met betrekking tot de resultaten van zijn werkzaamheden. Tevens maakt het de overeenkomstig artikel 43 afgelegde belangenverklaringen openbaar. Deze vereisten gelden ook voor de nationale coördinatiecentra, de kennisgemeenschap en de strategische adviesgroep overeenkomstig het desbetreffende recht.
3. De raad van bestuur kan op voorstel van de uitvoerend directeur belanghebbenden toestemming geven om de uitvoering van activiteiten van het kenniscentrum te observeren.
4. Het kenniscentrum legt in het reglement van orde van de raad van bestuur van het kenniscentrum en van de strategische adviesgroep de praktische regelingen voor de toepassing van de in de leden 1 en 2 van dit artikel bedoelde transparantiebepalingen vast. Voor uit Horizon Europa gefinancierde acties houden deze regels en regelingen terdege rekening met Verordening (EU) 2021/695.

*Artikel 35***Genderevenwicht**

Bij de tenuitvoerlegging van deze verordening kiezen de Commissie, de lidstaten en andere stakeholders uit de instellingen en de particuliere sector bij het benoemen van kandidaten of het voordragen van vertegenwoordigers, waar mogelijk en met het oog op genderevenwicht, vertegenwoordigers uit verschillende kandidaten.

*Artikel 36***Beveiligingsvoorschriften voor de bescherming van gerubriceerde informatie en gevoelige niet-gerubriceerde informatie**

1. De raad van bestuur stelt, na goedkeuring door de Commissie, de veiligheidsregels van het kenniscentrum vast. In deze veiligheidsregels worden de beginselen en regels die zijn vastgelegd in de Besluiten (EU, Euratom) 2015/443 ⁽¹⁹⁾ en (EU, Euratom) 2015/444 ⁽²⁰⁾ van de Commissie, toegepast.
2. De leden van de raad van bestuur, de uitvoerend directeur, de externe deskundigen die deelnemen aan ad-hoc-werkgroepen en de personeelsleden van het kenniscentrum houden zich ook na het beëindigen van hun functie aan de geheimhoudingsplicht uit hoofde van artikel 339 VWEU.
3. Het kenniscentrum kan de nodige maatregelen nemen om de uitwisseling van voor zijn taken relevante informatie met de Commissie en de lidstaten en, indien van toepassing, de relevante instellingen, organen en instanties van de Unie, te vergemakkelijken. Voor elke daartoe gesloten administratieve regeling inzake het delen van gerubriceerde EU-informatie (EUCI) of, bij het ontbreken van een dergelijke regeling, voor elke uitzonderlijke ad-hocvrijgave van EUCI, is voorafgaande toestemming van de Commissie vereist.

*Artikel 37***Toegang tot documenten**

1. Verordening (EG) nr. 1049/2001 is van toepassing op de documenten die bij het kenniscentrum berusten.
2. De raad van bestuur stelt uiterlijk op 29 december 2021 regelingen voor de uitvoering van Verordening (EG) nr. 1049/2001 vast.
3. Tegen besluiten van het kenniscentrum uit hoofde van artikel 8 van Verordening (EG) nr. 1049/2001 kan een klacht bij de Europese Ombudsman worden ingediend op grond van artikel 228 VWEU of een beroep bij het Hof van Justitie van de Europese Unie worden ingesteld uit hoofde van artikel 263 VWEU.

*Artikel 38***Verslaglegging, evaluatie en toetsing**

1. Het kenniscentrum zorgt ervoor dat zijn activiteiten, met inbegrip van de activiteiten die door de nationale coördinatiecentra en het netwerk worden beheerd, onderworpen zijn aan permanent en systematisch toezicht en periodieke evaluatie. Het kenniscentrum zorgt ervoor dat de gegevens voor het toezicht op de uitvoering en de resultaten van de in artikel 4, lid 3, punt b), bedoelde financieringsprogramma's van de Unie efficiënt, doeltreffend en tijdig worden verzameld, en legt proportionele verslagleggingsvereisten op aan ontvangers van middelen van de Unie en de lidstaten. De conclusies van die evaluatie worden bekendgemaakt.
2. Zodra er voldoende informatie beschikbaar is over de uitvoering van deze verordening, maar in ieder geval uiterlijk 30 maanden na de in artikel 46, lid 4, bepaalde datum, stelt de Commissie een uitvoeringsverslag op met betrekking tot de activiteiten van het kenniscentrum, rekening houdend met de voorafgaande input van de raad van bestuur, de nationale coördinatiecentra en de kennissamenleving. De Commissie zendt dat uitvoeringsverslag uiterlijk op 30 juni 2024 aan het Europees Parlement en de Raad toe. Het kenniscentrum en de lidstaten verstrekken de Commissie de informatie die zij voor de opstelling van dat verslag nodig heeft.
3. Het in lid 2 bedoelde uitvoeringsverslag omvat een beoordeling van:
 - a) de prestatiecapaciteit van het kenniscentrum met betrekking tot zijn doelstellingen, mandaat en taken, en de samenwerking en coördinatie met andere stakeholders, in het bijzonder de nationale coördinatiecentra, de kennissamenleving en Enisa;

⁽¹⁹⁾ Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie (PB L 72 van 17.3.2015, blz. 41).

⁽²⁰⁾ Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

- b) de door het kenniscentrum bereikte resultaten ten aanzien van zijn opdracht, doelstellingen, mandaat en taken, en met name de efficiëntie van het kenniscentrum bij het coördineren van de middelen van de Unie en het bundelen van deskundigheid;
- c) de samenhang van de uitvoeringstaken met de agenda en het meerjarige werkprogramma;
- d) de coördinatie en samenwerking van het kenniscentrum met de programmacomités van Horizon Europa en het programma Digitaal Europa, met name voor het versterken van de samenhang en de synergie met de agenda, het jaarlijkse werkprogramma, het meerjarige werkprogramma, Horizon Europa en het programma Digitaal Europa;
- e) gezamenlijke acties.

4) Na de indiening van het in lid 2 bedoelde uitvoeringsverslag verricht de Commissie, rekening houdend met de voorafgaande input van de raad van bestuur, de nationale coördinatiecentra en de kennisgemeenschap, een evaluatie van het kenniscentrum. Die evaluatie verwijst naar of actualiseert, naargelang het geval, de in lid 3 van dit artikel bedoelde beoordelingen, en wordt verricht vóór het einde van de in artikel 47, lid 1, gespecificeerde periode, teneinde tijdig te bepalen of het aangewezen is de looptijd van het mandaat van het kenniscentrum na die periode te verlengen. Bij die evaluatie worden de juridische en administratieve aspecten van het mandaat van het kenniscentrum beoordeeld, evenals het potentieel om synergieën tot stand te brengen en versnippering over andere instellingen, organen en instanties van de Unie te vermijden.

Indien de Commissie van oordeel is dat de voortzetting van het kenniscentrum gezien zijn opdracht, doelstellingen, mandaat en taken gerechtvaardigd is, kan zij een wetgevingsvoorstel indienen om de in artikel 47 vastgelegde duur van het mandaat van het kenniscentrum te verlengen.

5. Op grond van de conclusies van het in lid 2 bedoelde uitvoeringsverslag kan de Commissie passende maatregelen treffen.

6. Het toezicht, de evaluatie, de uitfasering en de verlenging van de bijdrage uit Horizon Europa gebeuren overeenkomstig de artikelen 10, 50 en 52 van Verordening (EU) 2021/695 en de overeengekomen uitvoeringsregelingen.

7. Het toezicht, de verslaglegging en de evaluatie van de bijdrage uit het programma Digitaal Europa gebeuren overeenkomstig de bepalingen van de artikelen 24 en 25 van Verordening (EU) 2021/694.

8. In geval van ontbinding van het kenniscentrum verricht de Commissie binnen zes maanden na die ontbinding, en in ieder geval uiterlijk twee jaar na de start van de in artikel 47 bedoelde ontbindingsprocedure, een eindevaluatie van het kenniscentrum. De resultaten van die eindevaluatie worden bij het Europees Parlement en bij de Raad ingediend.

Artikel 39

Rechtspersoonlijkheid van het kenniscentrum

1. Het kenniscentrum heeft rechtspersoonlijkheid.
2. In elke lidstaat bezit het kenniscentrum de ruimste handelingsbevoegdheid die door de wetgeving van de betrokken lidstaat aan rechtspersonen wordt verleend. Het kan met name roerende en onroerende goederen verkrijgen of vreemden en in rechte optreden.

Artikel 40

Aansprakelijkheid van het kenniscentrum

1. De contractuele aansprakelijkheid van het kenniscentrum valt onder het recht dat van toepassing is op de overeenkomst, het besluit of het contract in kwestie.
2. In geval van niet-contractuele aansprakelijkheid vergoedt het kenniscentrum alle schade die door zijn personeelsleden bij de uitoefening van hun taken is veroorzaakt, overeenkomstig de algemene beginselen die de wetgevingen van de lidstaten gemeen hebben.
3. Elke betaling door het kenniscentrum in verband met de aansprakelijkheid als bedoeld in de leden 1 en 2 en de daarmee verband houdende kosten en uitgaven worden beschouwd als uitgaven van het kenniscentrum en worden door zijn middelen gedekt.
4. Het kenniscentrum is als enige verantwoordelijk voor het nakomen van zijn verplichtingen.

*Artikel 41***Bevoegdheid van het Hof van Justitie van de Europese Unie en toepasselijk recht**

1. Het Hof van Justitie van de Europese Unie is bevoegd uitspraak te doen:
 - a) krachtens een arbitragebeding in door het kenniscentrum genomen besluiten of door het kenniscentrum aangegane overeenkomsten of contracten;
 - b) in geschillen over de vergoeding van schade die door personeelsleden van het kenniscentrum wordt veroorzaakt bij de uitoefening van hun taken;
 - c) in elk geschil tussen het kenniscentrum en zijn personeelsleden binnen de grenzen van en onder de voorwaarden vastgelegd in het Statuut.
2. In alle aangelegenheden die niet bij deze verordening of bij andere rechtshandelingen van de Unie zijn geregeld, is het recht van de lidstaat waar de zetel van het kenniscentrum zich bevindt, van toepassing.

*Artikel 42***Aansprakelijkheid van de Unie en de lidstaten en verzekering**

1. De financiële aansprakelijkheid van de Unie en de lidstaten voor de schulden van het kenniscentrum is beperkt tot de door hen reeds betaalde bijdrage aan de administratieve kosten.
2. Het kenniscentrum sluit de nodige verzekeringen af en houdt deze aan.

*Artikel 43***Belangenconflicten**

De raad van bestuur stelt regels vast om belangenconflicten met betrekking tot zijn leden, zijn organen en zijn personeel, inclusief de uitvoerend directeur, te voorkomen, vast te stellen en op te lossen. Deze regels omvatten de bepalingen ter voorkoming van belangenconflicten met betrekking tot de vertegenwoordigers van de leden die zitting hebben in de raad van bestuur en de strategische adviesgroep, overeenkomstig het Financieel Reglement, waaronder bepalingen betreffende belangenverklaringen. Voor de nationale coördinatiecentra geldt wat betreft belangenconflicten het nationale recht.

*Artikel 44***Bescherming van persoonsgegevens**

1. Op de verwerking van persoonsgegevens door het kenniscentrum is Verordening (EU) 2018/1725 van toepassing.
2. De raad van bestuur stelt uitvoeringsvoorschriften als bedoeld in artikel 45, lid 3, van Verordening (EU) 2018/1725 vast. De raad van bestuur kan aanvullende maatregelen vaststellen met het oog op de toepassing van die verordening door het kenniscentrum.

*Artikel 45***Ondersteuning door de gastlidstaat**

Tussen het kenniscentrum en de gastlidstaat waar zich de zetel van het centrum bevindt, kan een administratieve overeenkomst worden gesloten betreffende voorrechten, immuniteiten en andere ondersteuning die door die lidstaat aan het kenniscentrum worden verleend.

*HOOFDSTUK VI***Slotbepalingen***Artikel 46***Initiële acties**

1. De Commissie is belast met de oprichting en de initiële werking van het kenniscentrum totdat het over voldoende operationele capaciteit beschikt om zijn eigen begroting uit te voeren. Overeenkomstig het recht van de Unie betreft de Commissie de bevoegde organen van het kenniscentrum bij de uitvoering van alle nodige maatregelen.
2. Voor de toepassing van lid 1 van dit artikel kan de Commissie een tijdelijke uitvoerend directeur aanstellen, totdat de uitvoerend directeur zijn taken opneemt na zijn benoeming door de raad van bestuur overeenkomstig artikel 16. De tijdelijk uitvoerend directeur voert de taken van de uitvoerend directeur uit en kan worden bijgestaan door een beperkt aantal personeelsleden van de Commissie. De Commissie kan tijdelijk een beperkt aantal van haar personeelsleden aan het kenniscentrum toewijzen.

3. De tijdelijk uitvoerend directeur kan alle betalingen binnen de kredieten van de jaarbegroting van het kenniscentrum goedkeuren wanneer deze is aangenomen door de raad van bestuur, en kan overeenkomsten en contracten sluiten, met inbegrip van personeelscontracten, en besluiten aannemen, nadat de in artikel 13, lid 3, punt l), bedoelde personeelsformatie is vastgesteld.

4. De tijdelijk uitvoerend directeur bepaalt in samenspraak met de uitvoerend directeur en na goedkeuring door de raad van bestuur vanaf welke datum het kenniscentrum de capaciteit zal hebben om zijn begroting uit te voeren. Vanaf dat moment onthoudt de Commissie zich van het aangaan van verbintenissen en het uitvoeren van betalingen voor de activiteiten van het kenniscentrum.

Artikel 47

Duur

1. Het kenniscentrum wordt opgericht voor de periode van 28 juni 2021 tot en met 31 december 2029.
2. Tenzij het mandaat van het kenniscentrum overeenkomstig artikel 38, lid 4, wordt verlengd, wordt de ontbindingsprocedure automatisch gestart aan het einde van de in lid 1 van dit artikel bedoelde periode.
3. Voor de uitvoering van de procedure tot ontbinding van het kenniscentrum benoemt de raad van bestuur een of meer vereffenaars die handelen volgens de besluiten van de raad van bestuur.
4. Wanneer het kenniscentrum wordt ontbonden, worden zijn activa gebruikt ter voldoening van zijn verplichtingen en voor de uitgaven in verband met zijn ontbinding. Een eventueel overschot wordt verdeeld over de Unie en de bijdragende lidstaten in verhouding tot hun financiële bijdragen aan het kenniscentrum. Een eventueel overschot dat de Unie toevalt, wordt teruggeboekt naar de begroting van de Unie.

Artikel 48

Inwerkingtreding

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

Gedaan te Brussel, 20 mei 2021.

Voor het Europees Parlement

De voorzitter

D.M. SASSOLI

Voor de Raad

De voorzitter

A.P. ZACARIAS