



Regeling van de Minister van Economische Zaken en Klimaat van 1 september 2023, nr. WJZ/34688808, tot wijziging van de Regeling nationale EZK- en LNV-subsidies en de Regeling openstelling EZK- en LNV-subsidies 2023 in verband met de invoering en openstelling van de subsidiemodule cyberbeveiligingsinnovatieprojecten

De Minister van Economische Zaken en Klimaat

Gelet op de artikelen 2, eerste lid, 4, onderdelen a, b, c, d en h, 5, eerste en tweede lid, 16, 17, eerste lid, onderdeel a, 19, tweede en derde lid, 25, 34, eerste lid, 44 en 50, tweede lid, van het Kaderbesluit nationale EZK- en LNV-subsidies;

Besluit:

ARTIKEL I

De Regeling nationale EZK- en LNV-subsidies wordt als volgt gewijzigd:

A

In artikel 1.1 worden in de alfabetische volgorde de volgende begripsbepalingen ingevoegd, luidende:

grote onderneming: grote onderneming als bedoeld in artikel 2, onderdeel 24, van de algemene groepsvrijstellingsverordening;
organisatie-innovatie: organisatie-innovatie als bedoeld in artikel 2, onderdeel 96, van de algemene groepsvrijstellingsverordening;
procesinnovatie: procesinnovatie als bedoeld in artikel 2, onderdeel 97, van de algemene groepsvrijstellingsverordening;.

B

In artikel 3.27.1 vervallen de begripsbepalingen 'grote onderneming', 'organisatie-innovatie' en 'procesinnovatie'.

C

Na titel 4a.2 wordt een titel ingevoegd, luidende:

Titel 4a.3. Cyberbeveiligingsinnovatieprojecten

Artikel 4a.3.1. Begripsbepalingen

In deze titel wordt verstaan onder:

cyberbeveiliging: cyberbeveiliging als bedoeld in artikel 2, onderdeel 9, van verordening (EU) 2021/694;

Europees samenwerkingsverband: een samenwerkingsverband van onafhankelijke juridische entiteiten, die voldoen aan de voorwaarden, bedoeld in artikel 18 van verordening (EU) 2021/694;

juridische entiteit: juridische entiteit als bedoeld in artikel 2, onderdeel 2, van verordening (EU) 2021/694;

Nederlands samenwerkingsverband: een samenwerkingsverband van in Nederland gevestigde onafhankelijke juridische entiteiten;

onderzoeksorganisatie: organisatie voor onderzoek en kennisverspreiding als bedoeld in artikel 2, onderdeel 83, van de algemene groepsvrijstellingsverordening en paragraaf 1.3, onderdeel ee, van het O&O&l-steunkader;

verordening (EU) 2021/694: verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PbEU 2021 L 166/1).



Artikel 4a.3.2. Subsidieverstrekking

1. De Minister verstrekt op aanvraag subsidie voor het uitvoeren van een cyberbeveiligingsinnovatieproject dat gericht is op de verwezenlijking van één of meer van de operationele doelstellingen als bedoeld in artikel 6, eerste lid, van verordening (EU) 2021/694 op de volgende deelgebieden:
 - a. automatisering van cyberbeveiligingsoplossingen, waaronder mede begrepen het ontwikkelen van vernieuwende methoden of technieken en verspreiden van kennis over de automatisering van cyberbeveiligingsoplossingen;
 - b. het behoud en de ontwikkeling van personeel, waaronder mede begrepen het verbeteren en ontwikkelen van vernieuwende programma's betreffende het behoud en de ontwikkeling van personeel;
 - c. het proportioneel, veilig en privacybeschermend delen van data, waaronder mede begrepen het ontwikkelen van vernieuwende methoden of technieken voor proportioneel, veilig en privacybeschermend delen van data;
 - d. het doorontwikkelen of opschalen van bestaande cyberbeveiligingsoplossingen, waaronder mede begrepen het toepassen van vernieuwende methoden en technieken in het belang van de nationale veiligheid of voor nieuwe marktsegmenten.
2. Een cyberbeveiligingsinnovatieproject bevat een samenhangend geheel van activiteiten, waarbij een onderscheid gemaakt kan worden tussen:
 - a. niet-economische activiteiten, die kunnen bestaan uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling of een haalbaarheidsstudie, onafhankelijk uitgevoerd met het oog op meer kennis en een beter inzicht door een juridische entiteit die als onderzoeksorganisatie kwalificeert; of
 - b. economische activiteiten, die kunnen bestaan uit industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie of proces- en organisatie-innovatie, uitgevoerd door een juridische entiteit die voor het uitvoeren van deze activiteiten als onderneming kwalificeert.
3. De subsidieontvanger is een in Nederland gevestigde juridische entiteit, die:
 - a. niet kwalificeert als een natuurlijk persoon als bedoeld in artikel 18, derde lid, van verordening (EU) 2021/694;
 - b. de activiteiten, bedoeld in het tweede lid, zelfstandig dan wel in een Nederlands of Europees samenwerkingsverband uitvoert;
 - c. gedurende het indienen van de aanvraag om subsidie, bedoeld in artikel 4a.3.12, en het uitvoeren van de activiteiten, bedoeld in het tweede lid, niet verbonden is in een groep met één of meer andere juridische entiteiten die niet zijn gevestigd in één van de landen als bedoeld in artikel 18 van verordening (EU) 2021/694; en
 - d. voor zover deze een verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, heeft overgelegd, ten behoeve van de uitvoering van de economische activiteiten, bedoeld in het tweede lid, onderdeel b, geen onderneming in stand houdt die actief is in:
 - 1°. de sector visserij en aquacultuur;
 - 2°. de primaire productie van landbouwproducten; of
 - 3°. de sector verwerking en afzet van landbouwproducten in de gevallen, bedoeld in artikel 1, eerste lid, onder c, van de algemene de-minimisverordening.

Artikel 4a.3.3. Hoogte subsidie

1. De subsidie bedraagt voor een cyberbeveiligingsinnovatieproject:
 - a. voor niet-economische activiteiten door een juridische entiteit die kwalificeert als onderzoeksorganisatie: 100% van de subsidiabele kosten, voor zover deze betrekking hebben op fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling of een haalbaarheidsstudie;
 - b. voor economische activiteiten door een juridische entiteit die kwalificeert als een onderneming die een verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, heeft overgelegd: 100% van de subsidiabele kosten, voor zover deze betrekking hebben op industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie of proces- en organisatie-innovatie, met dien verstande dat het totale bedrag aan de-minimissteun per subsidieontvanger niet meer bedraagt dan het maximumbedrag, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening;
 - c. voor economische activiteiten door een juridische entiteit die kwalificeert als een onderneming die geen verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, heeft overgelegd:



- 1°. 50% van de subsidiabele kosten, voor zover deze betrekking hebben op industrieel onderzoek;
 - 2°. 25% van de subsidiabele kosten, voor zover deze betrekking hebben op experimentele ontwikkeling;
 - 3°. 50% van de subsidiabele kosten, voor zover deze betrekking hebben op een haalbaarheidsstudie;
 - 4°. 15% van de subsidiabele kosten, voor zover deze betrekking hebben op proces- en organisatie-innovatie door een grote onderneming;
 - 5°. 50% van de subsidiabele kosten, voor zover deze betrekking hebben op proces- en organisatie-innovatie door een middelgrote of kleine onderneming.
2. De percentages genoemd in het eerste lid, onderdeel c, subonderdelen 1°, 2° en 3°, worden opgehoogd met 10 procentpunten, indien de juridische entiteit kwalificeert als een middelgrote of kleine onderneming en de subsidiabele kosten worden gemaakt en betaald door deze middelgrote respectievelijk kleine onderneming.
 3. De subsidie per cyberbeveiligingsinnovatieproject bedraagt ten hoogste € 75.000.

Artikel 4a.3.4. Subsidiabele kosten

Voor subsidie komen uitsluitend in aanmerking de volgende kosten die verbonden zijn met de uitvoering van een niet-economische of economische activiteit:

- a. de kosten, bedoeld in artikel 25, derde lid, van de algemene groepsvrijstellingsverordening, voor zover deze betrekking hebben op fundamenteel onderzoek, industrieel onderzoek of experimentele ontwikkeling;
- b. de kosten, bedoeld in artikel 25, vierde lid, van de algemene groepsvrijstellingsverordening, voor zover deze betrekking hebben op een haalbaarheidsstudie;
- c. de kosten, bedoeld in artikel 29, derde lid, van de algemene groepsvrijstellingsverordening, voor zover deze betrekking hebben op proces- en organisatie-innovatie.

Artikel 4a.3.5. Verdeling van het subsidieplafond

De Minister verdeelt het subsidieplafond op volgorde van binnenkomst van de aanvragen.

Artikel 4a.3.6. Start- en Realisatietermijn

1. Met de uitvoering van een op grond van deze titel gesubsidieerd cyberbeveiligingsinnovatieproject wordt gestart voor 1 februari 2024.
2. De termijn, bedoeld in artikel 23, onderdeel b, van het besluit, is zes maanden.

Artikel 4a.3.7. Afwijzingsgronden

De Minister beslist afwijzend op een aanvraag indien:

- a. het cyberbeveiligingsinnovatieproject naar verwachting in onvoldoende mate bijdraagt aan de operationele doelstellingen op de deelgebieden, bedoeld in artikel 4a.3.2, eerste lid;
- b. de kwaliteit van het projectplan van het cyberbeveiligingsinnovatieproject onvoldoende is, blijkend uit de uitwerking van de beoogde resultaten, aanpak en methodiek, de financiële onderbouwing, de wijze waarop omgegaan wordt met risico's voor de succesvolle uitvoering van het cyberbeveiligingsinnovatieproject of de uitvoerbaarheid;
- c. de subsidiabele kosten onevenredig zijn ten opzichte van de beoogde resultaten van het cyberbeveiligingsinnovatieproject, omdat blijkt dat de beschikbare middelen onvoldoende effectief of efficiënt worden ingezet;
- d. de voor de uitvoering van het cyberbeveiligingsinnovatieproject benodigde competenties in onvoldoende mate aanwezig zijn binnen de subsidieaanvrager die het cyberbeveiligingsinnovatieproject uitvoert;
- e. de verwachte impact van het cyberbeveiligingsinnovatieproject op de markt en maatschappij onvoldoende is, blijkend uit de omstandigheid dat:
 - 1°. de verwachte toepassingsmogelijkheden en slaagkans van de met het project te ontwikkelen innovatie of innovaties voor de Nederlandse en internationale markt onvoldoende zijn; of
 - 2°. het verwachte draagvlak voor het cyberbeveiligingsinnovatieproject binnen in Nederland gevestigde ondernemingen, maatschappelijke organisaties of overheden onvoldoende is;
- f. de verwachte impact van het cyberbeveiligingsinnovatieproject op in Nederland gevestigde middelgrote of kleine ondernemingen onvoldoende is, omdat blijkt dat:

- 1°. er niet ten minste één middelgrote of kleine onderneming deelneemt aan het cyberbeveiligingsinnovatieproject; of
- 2°. er geen toepassingsmogelijkheden zijn van de ontwikkelde producten of diensten binnen de organisatie van middelgrote of kleine ondernemingen;
- g. de te verlenen subsidie minder dan € 25.000 per subsidieaanvrager zou bedragen;
- h. de aanvraag, voor zover deze aanvraag is ingediend door een subsidieaanvrager die een verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, heeft overgelegd, activiteiten bevat die direct verband houden met:
 - 1°. de omvang van de uitvoer naar andere lidstaten van de Europese Unie of derde landen;
 - 2°. het oprichten en exploiteren van een distributienet ten behoeve van de uitvoer; of
 - 3°. andere lopende uitgaven direct verband houdend met activiteiten op het gebied van uitvoer.

Artikel 4a.3.9. Verplichtingen betreffende niet-economische activiteiten door een onderzoeksorganisatie

1. Indien in het cyberbeveiligingsinnovatieproject niet-economische activiteiten door een onderzoeksorganisatie worden verricht, worden deze projectactiviteiten in de boekhouding opgenomen als niet-economische activiteiten.
2. Indien in het cyberbeveiligingsinnovatieproject niet-economische activiteiten door een onderzoeksorganisatie worden verricht in een samenwerkingsverband:
 - a. wordt voorafgaand aan de start van het cyberbeveiligingsinnovatieproject een samenwerkingsovereenkomst gesloten tussen de deelnemers aan het samenwerkingsverband over de wijze waarop wordt omgegaan met de bijdrage in de kosten, het delen in de risico's en uitkomsten, de verspreiding van de resultaten en de toegang tot en de regels voor de toewijzing van intellectuele eigendomsrechten;
 - b. worden de projectactiviteiten door de onderzoeksorganisatie uitgevoerd in daadwerkelijke samenwerking met ondernemingen; en
 - c. draagt de onderzoeksorganisatie er zorg voor dat:
 - 1°. De deelnemende ondernemingen de volledige kosten van de activiteiten dragen;
 - 2°. De resultaten van de activiteiten waaraan geen intellectuele eigendomsrechten kunnen worden ontleend, ruim mogen worden verspreid en eventuele intellectuele eigendomsrechten die uit de activiteiten van het onderzoeksorganisatie voortvloeien, volledig aan haar worden toegekend;
 - 3°. Uit de activiteiten ontstane intellectuele eigendomsrechten, alsmede daarmee verband houdende toegangsrechten, aan de verschillende samenwerkende deelnemers worden toegekend op een wijze die een passende afspiegeling is van hun werkpakketten, bijdragen en respectieve belangen; of
 - 4°. Deze van de deelnemende ondernemingen een vergoeding ontvangt die overeenstemt met de marktprijs voor de intellectuele eigendomsrechten die voortvloeien uit het samenwerkingsproject die worden overgedragen aan de deelnemende ondernemingen.
3. Het absolute bedrag van financiële en niet-financiële bijdragen van de deelnemende ondernemingen in de kosten van de activiteiten van de onderzoeksorganisatie die de betrokken intellectuele eigendomsrechten hebben opgeleverd, kan op de vergoeding, bedoeld in het tweede lid, onderdeel c, subonderdeel 4°, in mindering worden gebracht.
4. De vergoeding, bedoeld in het tweede lid, onderdeel c, subonderdeel 4°, stemt overeen met de marktprijs indien:
 - a. het bedrag van de vergoeding is vastgesteld via een publieke, open en transparante concurrerende verkoopprocedure;
 - b. een taxatie van een onafhankelijke deskundige bevestigt dat de prijs overeenstemt met de marktprijs;
 - c. de onderzoeksorganisatie als verkoper kan aantonen dat zij heeft onderhandeld over de vergoeding, om rekening houdende met haar algemene doelstellingen, maximaal economisch voordeel te behalen op het tijdstip dat de overeenkomst betreffende de vergoeding wordt afgesloten; of
 - d. in de gevallen waarin de samenwerkingsovereenkomst, bedoeld in het tweede lid, onderdeel a, de onderneming een voorkeursrecht geeft ten aanzien van het door de onderzoeksorganisatie gegenereerde intellectuele eigendomsrecht, wanneer hieraan voor de onderzoeksorganisatie het recht is gekoppeld derden te verzoeken om economisch meer voordelige aanbiedingen, zodat de onderneming haar aanbod daaraan moet aanpassen.
5. De voorwaarden van een overeenkomst, gesloten ingevolge het vierde lid, onderdeel c, wijken niet af van voorwaarden die onafhankelijke ondernemingen overeen zouden komen en



behelzen geen enkele vorm van heimelijke verstandhouding.

6. Artikel 1.9 is niet van toepassing op deze titel.

Artikel 4a.3.10. Verplichtingen betreffende proces- en organisatie-innovatie door een grote onderneming

Indien in het cyberbeveiligingsinnovatieproject activiteiten betreffende proces- en organisatie-innovatie door een grote onderneming worden verricht, worden deze projectactiviteiten door de grote onderneming uitgevoerd in daadwerkelijke samenwerking met middelgrote en kleine ondernemingen, die ten minste 30% van de totale subsidiabele kosten dragen.

Artikel 4a.3.11. Verplichtingen betreffende voorlichting

Gedurende twee jaar na de datum van de beschikking tot subsidievaststelling maakt de subsidieontvanger na afloop van het onderzoeksproject de niet bedrijfsgevoelige kennis en informatie die met het op grond van deze titel gesubsidieerde cyberinnovatieproject wordt opgedaan openbaar:

- a. via daarvoor geschikte conferenties, publicaties, open access-repositories dan wel gratis of opensource-software als bedoeld in artikel 25, zesde lid, onderdeel b, subonderdeel II, van de algemene groepsvrijstellingsverordening; en
- b. voor zover van toepassing, via een op verzoek van en naar het oordeel van de Minister opgesteld:
 - 1°. kwalitatief voldoende verslag, dat wordt verstrekt met gebruikmaking van een middel dat door de Minister beschikbaar wordt gesteld; of
 - 2°. adequaat voorlichtingsmateriaal, dat wordt gepresenteerd tijdens een geschikte conferentie.

Artikel 4a.3.12. Informatieverplichtingen

1. Onverminderd het eerste lid bevat een aanvraag om subsidie ten minste:
 - a. gegevens over de subsidieaanvrager, waaronder het post- en bezoekadres, het rekeningnummer en, voor zover van toepassing, het nummer waarmee de subsidieaanvrager is geregistreerd bij de Kamer van Koophandel;
 - b. gegevens over de contactpersoon bij de subsidieaanvrager, waaronder de naam, het telefoonnummer en het e-mailadres;
 - c. kerngegevens over het cyberbeveiligingsinnovatieproject, die bestaan uit een voor openbare publicatie geschikte samenvatting van de projectomschrijving en, voor zover van toepassing, een lijst met deelnemers in het Nederlandse of Europese samenwerkingsverband dat het cyberbeveiligingsinnovatieproject zal uitvoeren;
 - d. een verklaring de-minimissteun van de subsidieaanvrager, indien de subsidieaanvrager aanspraak wil maken op het percentage aan subsidie, bedoeld in artikel 4a.3.3, eerste lid, onderdeel b;
 - e. de gegevens, bedoeld in artikel 6, tweede lid, van de algemene groepsvrijstellingsverordening, indien de subsidieaanvrager aanspraak wil maken op het percentage aan subsidie, bedoeld in artikel 4a.3.3, eerste lid, onderdeel c;
 - f. gegevens over de grootte van de onderneming van de subsidieaanvrager, indien de subsidieaanvrager aanspraak wil maken op een verhoogd percentage aan subsidie voor een kleine of middelgrote onderneming als bedoeld in artikel 4a.3.3, tweede lid.
2. De aanvraag gaat vergezeld van:
 - a. een projectplan met daarin een projectomschrijving van de doelen, de deelgebieden en de activiteiten, bedoeld in artikel 4a.2.2, eerste en tweede lid, van het cyberbeveiligingsinnovatieproject;
 - b. een projectbegroting waarin per projectfase en deelnemer een omschrijving wordt gegeven van:
 - 1°. de omvang van de gevraagde subsidie;
 - 2°. de totale subsidiabele kosten van het cyberbeveiligingsinnovatieproject en op welke activiteiten als bedoeld in artikel 4a.3.2, tweede lid, deze kosten betrekking hebben;
 - c. een beknopte beschrijving van de competenties van de bij de uitvoering van het cyberbeveiligingsinnovatieproject betrokken organisaties of personen;
 - d. een beknopte beschrijving van de strategie en ontwikkelprioriteiten van de subsidieaanvrager en op welke termijn het te ontwikkelen product of dienst de markt naar verwachting zal bereiken en welke impact het daar zal hebben;
 - e. voor zover van toepassing, een samenwerkingsovereenkomst als bedoeld in artikel 4a.3.9, tweede lid, onderdeel a;
 - f. een door de Minister beschikbaar gesteld ingevuld formulier, waaruit volgt dat de subsidie-



aanvrager niet in een groep verbonden is met één of meer andere juridische entiteiten die niet zijn gevestigd in één van de landen als bedoeld in artikel 18 van verordening (EU) 2021/694.

Artikel 4a.3.13. Aanvraag subsidievaststelling

Het eindverslag, bedoeld in artikel 50, tweede lid, onderdeel a, van het besluit, waarvan de aanvraag tot subsidievaststelling vergezeld gaat, bevat in ieder geval:

- a. een omschrijving van de projectresultaten van het cyberbeveiligingsinnovatieproject;
- b. op welke wijze het cyberbeveiligingsinnovatieproject heeft bijgedragen aan de doelen en deelgebieden, bedoeld in artikel 4a.3.2, eerste lid.

Artikel 4a.3.14. Staatssteun

De subsidie, bedoeld in artikel 4a.3.2, eerste lid, met uitzondering van de subsidie voor niet-economische activiteiten, bedoeld in artikel 4a.3.2, tweede lid, onderdeel a, bevat staatsteun en wordt gerechtvaardigd door:

- a. de algemene de-minimisverordening, indien de subsidieaanvrager aanspraak wil maken op het percentage aan subsidie, bedoeld in artikel 4a.3.3, eerste lid, onderdeel b;
- b. de artikelen 25 en 29 van de algemene groepsvrijstellingsverordening, indien de subsidieaanvrager aanspraak wil maken op de percentages aan subsidie als bedoeld in artikel 4a.3.3, eerste lid, onderdeel c, of tweede lid.

Artikel 4a.3.15. Vervaltermijn

Deze titel vervalt met ingang van 1 oktober 2028, met dien verstande dat deze van toepassing blijven op subsidies die voor deze datum zijn verleend.

ARTIKEL II

In de tabel van artikel 1 van de Regeling openstelling EZK- en LNV-subsidies 2023 wordt na titel 4a.2 een rij ingevoegd, luidende:

Titel 4a.3: Cyberbeveiligingsinnovatieprojecten				02-10-2023 t/m 02-11-2023	€ 930.000
---	--	--	--	------------------------------	-----------

ARTIKEL III

Deze regeling treedt in werking met ingang van 1 oktober 2023.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

's-Gravenhage, 1 september 2023

*De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens*



TOELICHTING

I. Algemeen

1. Aanleiding, doel en inhoud

Met deze regeling wordt de subsidiemodule Cyberbeveiligingsinnovatieprojecten ingevoerd en opgesteld.

1.1 Aanleiding

Binnen de diverse lidstaten van de Europese Unie wordt steeds meer gesteund op digitale technologieën. Hierdoor worden burgers en bedrijven binnen de Europese Unie steeds meer blootgesteld aan ernstige cyberbeveiligingsincidenten (onder meer in de vorm van ernstige verstoringen van netwerk- en informatiesystemen), die gevolgen hebben voor individuele lidstaten van de Europese Unie en voor de Europese Unie als geheel. Een hoge mate van beveiliging van netwerk- en informatiesystemen in de hele Europese Unie is dan ook essentieel zowel voor de maatschappij als voor de economie. Om die reden is er binnen de Europese Unie behoefte aan (grotere) cyberweerbaarheid, grotere technologische en industriële vermogens, hoge cyberbeveiligingsnormen en holistische cyberbeveiligingsoplossingen.

Voor cyberbeveiliging is de Europese Unie echter (teveel) afhankelijk van niet-Europese aanbieders. Het is dan ook in het strategisch belang van de Europese Unie om essentiële onderzoeks- en technologische capaciteiten op het gebied van cyberbeveiliging te behouden en te ontwikkelen ten behoeve van de bescherming van (vitale) netwerk- en informatiesystemen (van burgers en bedrijven). Daarbij is het gewenst om alle versnipperde inspanningen, ervaringen en deskundigheid op een efficiënte manier te bundelen en in een netwerk onder te brengen.

Met verordening (EU) 2021/887¹ is in deze bundeling voorzien via de oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (hierna: EKC). Het EKC moet specifieke taken uitvoeren met betrekking tot industrie, technologie en onderzoek op het gebied van cyberbeveiliging. Deze taken bestaan onder meer uit het beheer en de verstrekking van financiële middelen uit verschillende Europese programma's, zoals uit het programma Digitaal Europa, vastgesteld bij verordening (EU) 2021/694²³. Deze financiële middelen kunnen door het EKC (onder meer via het openstellen van calls) verstrekt worden aan een zogenaamd Nationaal Coördinatiecentrum (hierna: NCC). Zo heeft de EKC onder meer de call 'Cybersecurity and Trust (DIGITAL-2022-CYBER-02)'⁴ opgesteld, waaruit na selectie van de projectvoorstellen door het EKC onder meer financiële middelen verstrekt zijn aan het Nederlandse NCC⁵ (hierna: NCC.NL), onderdeel van het Ministerie van Economische Zaken en Klimaat. Deze financiële middelen zijn bestemd voor de subsidieverstrekking onder de subsidiemodule Cyberbeveiligingsinnovatieprojecten⁶, die met onderhavige regeling is ingevoerd.

Met Europese en Nederlandse cofinanciering (van ieder 50 procent van het subsidiebedrag) wordt op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten subsidie verstrekt voor het uitvoeren van een cyberbeveiligingsinnovatieproject door een in Nederland gevestigde juridische entiteit, die (a) niet kwalificeert als natuurlijke persoon en (b) de activiteiten van het project zelfstandig dan wel in een Nederlands of Europees samenwerkingsverband uitvoert. Een cyberbeveiligingsinnovatieproject bevat een samenhangend geheel van activiteiten, dat kan bestaan uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie of proces- en organisatie-innovatie. Ook moeten de cyberbeveiligingsinnovatieprojecten voldoen aan de Europese doelstellingen op de deelgebieden, zoals omschreven in paragraaf 1.2 van de algemene toelichting.

¹. 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 (PbEU 2021 L 202).

². Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PbEU 2021 L 166/1).

³. Voor de financiering onder het Programma Digitaal Europa kwalificeert het EKC (op grond van overweging 23 van verordening (EU)2021/887) als een zogenaamd Europees partnerschap als bedoeld in artikel 2, onderdeel 7, van verordening (EU) 2021/694, die via (onder meer) het Programma Digitaal Europa financiële middelen beschikbaar kan stellen aan een zogenaamd nationaal coördinatiecentrum (hierna: NCC).

⁴. De call 'Cybersecurity and Trust (DIGITAL-2022-CYBER-02)' is te raadplegen via <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination>.

⁵. Zie <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101100801/DIGITAL>

⁶. Zie <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101100801/DIGITAL>



1.2 Doelstellingen

Met deze regeling wordt de subsidiemodule Cyberbeveiligingsinnovatieprojecten ingevoerd in titel 4.a.3 van de Regeling nationale EZK- en LNV-subsidies. Hiermee wordt beoogd om subsidie te verstrekken voor het uitvoeren van cyberbeveiligingsinnovatieprojecten die gericht zijn op het verwezenlijken van de Europese en Nederlandse (maatschappelijke) doelstellingen op het gebied van cyberbeveiliging, neergelegd in onder meer het Programma Digitaal Europa (verordening (EU) 2021/694).

Allereerst bevat het programma Digitaal Europa algemene doelstellingen, die zijn opgenomen in artikel 3, eerste lid, van verordening (EU) 2021/694. Deze algemene doelstellingen zijn gericht op het ondersteunen en versnellen van de digitale transformatie van de economie, het bedrijfsleven en de samenleving in de Europese Unie, waarvan burgers, overheden en bedrijven in de hele Europese Unie zouden moeten kunnen profiteren. Daarbij is het doel het verbeteren van het concurrentievermogen van de Europese Unie in de mondiale digitale economie. Tegelijkertijd is het doel de digitale kloof in de hele Europese Unie te helpen overbruggen en de strategische autonomie van de Europese Unie te versterken door een holistische, sector- en grensoverschrijdende steun en een grotere bijdrage van de Europese Unie. Voor de verwezenlijking van deze doelstellingen is van belang dat het Programma Digitaal Europa wordt uitgevoerd in nauwe coördinatie met andere toepasselijke programma's van de Europese Unie en gericht zal zijn op: (a) het versterken en bevorderen van de capaciteiten van Europa op belangrijke gebieden van de digitale technologie door middel van grootschalige uitrol en (b) in de private sector en op gebieden van algemeen belang, het verruimen van de verspreiding en het gebruik van de belangrijkste digitale technologieën van Europa, waarbij de digitale transformatie van deze capaciteiten en de toegang tot digitale technologieën worden bevorderd.

Verder bevat het Programma Digitaal Europa vijf onderling samenhangende specifieke doelstellingen, die zijn neergelegd in artikel 3, tweede lid, van verordening (EU) 2021/694. Met de subsidie aan cyberbeveiligingsinnovatieprojecten moet een bijdrage worden geleverd aan specifieke doelstelling 3 (cyberbeveiliging en vertrouwen) als bedoeld in artikel 3, tweede lid, onderdeel c, van verordening (EU) 2021/694, en dan met name de volgende hieraan gekoppelde operationele doelstellingen, opgenomen in artikel 6 van verordening (EU) 2021/694:

- (a) de opbouw en aanschaf van geavanceerde apparatuur, instrumenten en data infrastructuur inzake cyberbeveiliging om op Europees niveau een hoog gemeenschappelijk niveau van cyberbeveiliging tot stand te brengen, met volledige naleving van de wetgeving inzake gegevensbescherming en van de grondrechten, en waarbij wordt gezorgd voor de strategische autonomie van de Europese Unie;
- (b) ondersteunen van de opbouw en het optimaal gebruik van Europese kennis, capaciteiten en vaardigheden in verband met cyberbeveiliging, en het delen en integreren van beste praktijken;
- (c) de brede uitrol van doeltreffende uiterst geavanceerde cyberbeveiligingsoplossingen in de hele Europese economie, met speciale aandacht voor overheidsinstanties en kleine en middelgrote ondernemingen;
- (d) versterken van de capaciteiten in de lidstaten van de Europese Unie en de private sector om hen te helpen te voldoen aan Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad, onder meer door maatregelen ter ondersteuning van het overnemen van beste praktijken op het gebied van cyberbeveiliging;
- (e) het vergroten van de weerbaarheid tegen cyberaanvallen, het helpen vergroten van het risicobewustzijn en de kennis over cyberbeveiligingsprocessen, en het ondersteunen van publieke en private organisaties bij het bereiken van basale cyberbeveiligingsniveaus via bijvoorbeeld invoering van eind-tot-eindversleuteling van gegevens en software-updates; en
- (f) verbeteren van de samenwerking tussen de civiele en de defensie-industrie met betrekking tot projecten, diensten, competenties en toepassingen voor tweërlei gebruik op het gebied van cyberbeveiliging, in overeenstemming met een verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra ('verordening kenniscentrum cyberbeveiliging').

Met de cyberbeveiligingsinnovatieprojecten die onder de subsidiemodule Cyberbeveiligingsinnovatieprojecten vallen zal (gedeeltelijk) invulling moeten worden gegeven aan de voorgaande operationele doelstellingen, onderdeel van specifieke doelstelling 3. De door het cyberbeveiligingsinnovatieproject geleverde bijdrage zal dan ook niet alles omvattend hoeven te zijn, maar concreet moeten in gaan op één of meer facetten van één of meer van de voorgaande operationele doelstellingen op één of meer deelgebieden, opgenomen in artikel 4a.3.2, eerste lid, onderdelen a, b, c en d.

1.3 Openstelling en verdeling van het subsidieplafond

Met deze wijzigingsregeling wordt de Regeling openstelling EZK- en LNV-subsidies 2023 aangepast, zodat de subsidiemodule Cyberbeveiligingsinnovatieprojecten opengesteld kan worden. Voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten loopt de openstellingsperiode van 2 oktober



2023 om 9.00 uur tot en met 2 november 2023 om 17.00 uur. Het subsidieplafond wordt vastgesteld op € 930.000.

2. Staatssteun

Op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten kan subsidie worden verstrekt aan een in Nederland gevestigde juridische entiteit, niet-zijnde een natuurlijk persoon, voor het zelfstandig of in een Europees samenwerkingsverband uitvoeren van een cyberbeveiligingsinnovatieproject dat een bijdrage moet leveren aan de doelen uit het programma Digitaal Europa zoals neergelegd in artikel 6, eerste lid, van verordening (EU) 2021/694. Het gaat hierbij om de invulling van de doelstellingen op een aantal deelgebieden.

2.1 Reikwijdte van de subsidie

De subsidie is bestemd voor een cyberbeveiligingsinnovatieproject dat een samenhangend geheel van activiteiten bevat. Deze subsidiabele activiteiten kunnen worden onderverdeeld in (a) niet-economische activiteiten en (b) economische activiteiten.

Niet-economische activiteiten (artikel 4a.3.2, tweede lid, onderdeel a)

De niet-economische activiteiten, bedoeld in artikel 4a.3.2, tweede lid, onderdeel a, kunnen bestaan uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling en/of een haalbaarheidsstudie en worden onafhankelijk uitgevoerd met het oog op meer kennis en een beter inzicht door een juridische entiteit die als onderzoeksorganisatie kwalificeert als bedoeld in artikel 2, onderdeel 83, van de algemene groepsvrijstellingsverordening en paragraaf 1.3, onderdeel ee, van het O&O&I-steunkader. De subsidie voor deze activiteiten bevat geen staatssteun. Hierop is dus geen steunkader en ook geen maximum steunintensiteit van toepassing. Er is daarom voor gekozen de steunintensiteit vast te stellen op een percentage van 100%, zodat een maximale stimulans aan de voormelde subsidiabele activiteiten wordt gegeven. Wel zijn de niet-economische activiteiten nader afgebakend. Voor wat al dan niet onder niet-economische activiteiten van onderzoeksorganisaties wordt verstaan, wordt aangesloten bij het zogenaamde O&O&I-steunkader⁷ op grond waarvan randvoorwaarden en waarborgen zijn opgenomen in de artikelen 4a.3.2, tweede lid, onderdeel a, en 4a.3.9.

Economische activiteiten (artikel 4a.3.2, tweede lid, onderdeel b)

De economische activiteiten, bedoeld in artikel 4a.3.2, tweede lid, onderdeel b, kunnen bestaan uit industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie en/of proces- en organisatie-innovatie, door een juridische entiteit die kwalificeert als onderneming als bedoeld in artikel 1 van het Kaderbesluit nationale EZK- en LNV-subsidies (hierna: Kaderbesluit). De subsidie voor deze activiteiten bevat staatssteun die wordt gerechtvaardigd door twee Europese staatssteunkaders.

Allereerst wordt de staatssteun aan economische activiteiten gerechtvaardigd door artikel 3 van de algemene de-minimisverordening⁸, in het geval de subsidieaanvrager ten behoeve van de subsidieverlening voor de uitvoering van deze economische activiteiten een verklaring de-minimissteun heeft verstrekt⁹ betreffende het niet-overschrijden van het de-minimisplafond, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening. Op de subsidie die door de algemene de-minimisverordening wordt gerechtvaardigd, is geen maximum steunintensiteit van toepassing. Er is daarom voor gekozen de steunintensiteit vast te stellen op een percentage van 100%, zodat in dit geval een maximale stimulans aan de voormelde subsidiabele economische activiteiten wordt gegeven. Wel zijn de economische activiteiten nader afgebakend en zijn op grond van de algemene de-minimisverordening randvoorwaarden en waarborgen opgenomen in de artikelen 4a.3.2, derde lid, onderdeel d, 4a.3.3, eerste lid, onderdeel b, 4a.3.7, onderdeel h, en 4a.3.12, eerste lid, onderdeel d. Hierdoor wordt ervoor gezorgd dat door de subsidieverstreking het de-minimisplafond, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening niet wordt overschreden en voldaan wordt aan de beperkingen betreffende steunverlening voor bepaalde activiteiten in bepaalde sectoren en/of in- en uitvoer.

Ten tweede wordt de staatssteun aan economische activiteiten gerechtvaardigd door de artikelen 25

⁷. Kaderregeling betreffende staatssteun voor onderzoek, ontwikkeling en innovatie nr. 2022/C 414/01 (PbEU 2022, C 414).

⁸. verordening (EU) nr. 1407/2013 van de Commissie van 18 december 2013 betreffende de toepassing van de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie op de de-minimissteun (PbEU 2013, L 352).

⁹. In artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies wordt een verklaring de-minimissteun omschreven als verklaring van de subsidieaanvrager waarin deze bevestigt dat subsidieverlening niet zal leiden tot een overschrijding van het de-minimisplafond, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening.



en 29 van de algemene groepsvrijstellingsverordening¹⁰, in het geval de subsidieaanvrager ten behoeve van de subsidieverlening voor de uitvoering van deze economische activiteiten geen verklaring de-minimissteun heeft verstrekt. Het deel van de subsidiabele kosten dat voor subsidie in aanmerking komt (de steunintensiteit) bedraagt bij industrieel onderzoek 50% voor grote ondernemingen en 60% voor middelgrote en kleine ondernemingen, bij experimentele ontwikkeling 25% voor grote ondernemingen en 35% voor middelgrote en kleine ondernemingen, bij een haalbaarheidsstudie 50% voor grote ondernemingen en 60% voor middelgrote en kleine ondernemingen en bij proces- en organisatie-innovatie 15% voor grote ondernemingen en 50% voor middelgrote en kleine ondernemingen. Deze percentages vallen binnen de marges van het toepasselijke staatssteunkader (artikelen 25 en 29 van de algemene groepsvrijstellingsverordening). Ook wordt gebleven onder de aanmeldingsdrempels opgenomen in artikel 4 van de algemene groepsvrijstellingsverordening. In de subsidiemodule Cyberbeveiligingsinnovatieprojecten wordt, waar nodig, verwezen naar de relevante basis in de algemene groepsvrijstellingsverordening. Hierbij is van belang dat ook de economische activiteiten nader zijn afgebakend en dat er op grond van de algemene groepsvrijstellingsverordening randvoorwaarden en waarborgen zijn opgenomen in de artikelen 4a.3.2, tweede lid, onderdeel b, 4a.3.3, tweede lid, onderdeel c, en tweede lid, 4a.3.10 en 4a.3.12, eerste lid, onderdelen e en f.

Voor een uitgebreidere omschrijving van de achtergrond en reikwijdte van de subsidiabele activiteiten, hoogte van de subsidie en subsidiabele kosten wordt verwezen naar de artikelsgewijze toelichting op de artikelen 4a.3.2, 4a.3.3, 4a.3.4, 4a.3.9, 4a.3.10 en 4a.3.12.

2.2 Transparantie, cumulatie, stimulerend effect en overige voorwaarden

De steunverlening op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten is aan randvoorwaarden onderworpen, zodat voldaan wordt aan de volgende voorwaarden van de algemene de-minimisverordening en algemene groepsvrijstellingsverordening.

Allereerst wordt met het maximumsubsidiebedrag, opgenomen in artikel 4a.3.3, derde lid, van deze regeling, gebleven onder zowel het toepasselijke de-minimisplafond, opgenomen in artikel 3, tweede lid, van de algemene de-minimisverordening als de toepasselijke aanmeldingsdrempels voor individuele subsidieverstreking, opgenomen in artikel 4, eerste lid, van de algemene groepsvrijstellingsverordening.

Verder wordt met artikel 22, eerste lid, onderdeel b, subonderdeel 1^o, van het Kaderbesluit, samen met artikelen 4a.3.3 en 4a.3.4, gewaarborgd dat de steun overeenkomstig artikel 4 van de algemene de-minimisverordening en artikel 5 van de algemene groepsvrijstellingsverordening transparant is. Ook waarborgen de artikelen 6, 7, 8 en 22, eerste lid, onderdeel b, subonderdeel 4^o, van het Kaderbesluit dat wordt voldaan aan de eisen betreffende cumulatie, opgenomen in artikel 5 van de algemene de-minimisverordening en artikel 8 van de algemene groepsvrijstellingsverordening.

Tot slot heeft de steun (overeenkomstig artikel 6 van de algemene groepsvrijstellingsverordening) een stimulerend effect, omdat de subsidiabele activiteiten pas zullen starten nadat de subsidieaanvraag is ingediend.

2.3 Kennisgeving en openbare bekendmaking van gegevens inzake steunverlening

Van de publicatie van de invoering van en openstelling van de subsidiemodule Cyberbeveiligingsinnovatieprojecten, alsook van toekomstige publicaties van wijzigingen en openstellingen van de subsidiemodule Cyberbeveiligingsinnovatieprojecten, zal een kennisgeving aan de Europese Commissie worden gedaan, conform artikel 11, onder a, van de algemene groepsvrijstellingsverordening. Omdat een subsidie die op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten wordt verleend, staatssteun bevat die onder meer door de algemene groepsvrijstellingsverordening wordt gerechtvaardigd, maakt de Minister van Economische Zaken en Klimaat (EZK) binnen zes maanden na de datum van subsidieverlening de gegevens, genoemd in artikel 1.8 van de Regeling nationale EZK- en LNV-subsidies, bekend.

3. Regeldruk

3.1 Algemeen

Deze regeling betreft de invoering van de subsidiemodule Cyberbeveiligingsinnovatieprojecten. Voor de administratieve lasten is van belang dat er sprake is van Europese cofinanciering. In tegenstelling tot bij andere subsidiemodules met Europese cofinanciering heeft EZK voor onderhavige subsidiemodule zelf het Europese proces doorlopen en op grond hiervan Europese financiering ontvangen, die EZK kan gebruiken voor de subsidieverlening onder de subsidiemodule Cyberbeveiligingsinnovatie-

¹⁰ Verordening (EU) nr. 651/2014 van de Commissie van 17 juni 2014 waarbij bepaalde categorieën steun op grond van de artikelen 107 en 108 van het Verdrag met de interne markt verenigbaar worden verklaard (PbEU 2014, L 187).



projecten. Deze subsidiemodule heeft administratieve lasten tot gevolg, samenhangend met de aanvraag voor subsidie en de aanvraag tot subsidievaststelling.

3.2 Informatieverplichtingen

Om voor subsidie in aanmerking te kunnen komen, moet een aanvraag om subsidieverlening (hierna: de subsidieaanvraag) worden ingediend waarin of waarbij bepaalde informatie verschaft moet worden. In artikel 4a.3.12 zijn informatieverplichtingen opgenomen ten aanzien van de gegevens die de subsidieaanvraag moet bevatten en van welke bescheiden deze vergezeld dient te gaan. Voor de subsidieaanvraag is een aantal minimale informatievereisten opgenomen over de subsidieaanvrager, het project en de (eventuele) andere deelnemers aan het project, die nodig zijn om de subsidieaanvraag te kunnen behandelen. Hiervoor wordt vanuit RVO.nl een aantal standaard formats aangeleverd dat ingevuld moeten worden. Daarnaast moet de subsidieaanvraag vergezeld gaan van een projectplan (met daarin een projectomschrijving van doelen, deelgebieden en de activiteiten) en een projectbegroting. Ook moet de subsidieaanvraag vergezeld gaan van een beknopte beschrijving van de competenties van de bij de uitvoering van het cyberbeveiligingsinnovatieproject betrokken organisaties of personen, alsook een beknopte beschrijving van de strategie en ontwikkelprioriteiten van de subsidieaanvrager, op welke termijn het te ontwikkelen product of dienst de markt naar verwachting zal bereiken en welke impact het daar zal hebben. Daarnaast dient de subsidieaanvraag vergezeld te gaan van een samenwerkingsovereenkomst en een ingevuld formulier waaruit volgt dat de subsidieaanvrager niet in een groep verbonden is met één of meer andere juridische entiteiten die niet zijn gevestigd in één van de landen als bedoeld in artikel 18 van verordening (EU) 2021/694. Al deze informatie is nodig voor de beoordeling van de subsidieaanvraag.

Na een positieve beoordeling van de subsidieaanvraag zal er subsidie verleend worden. Het Cyberbeveiligingsinnovatieproject moet uiterlijk gestart worden op 1 februari 2024 en afgerond zijn binnen zes maanden na de start hiervan. Gelet op de (korte) projectduur worden er geen tussentijdse (jaarlijkse) rapportage(s) over de voortgang opgevraagd op grond van artikel 39 van het Kaderbesluit. Alle informatie over het verloop van het project zal verstrekt moeten worden bij de uiteindelijke vaststelling van de subsidie.

Voor de vaststelling van de subsidie moet de subsidieontvanger een aanvraag tot subsidievaststelling indienen waarin deze (in beschikbare formulieren en in de vorm van een eindrapportage) informatie moet verschaffen. Voor de aanvraag tot subsidievaststelling zijn de informatieverplichtingen opgenomen in artikel 50 van het Kaderbesluit. Er is evenwel voor gekozen om deze informatieverplichtingen in artikel 4a.3.13 nader in en aan te vullen. Zo moet het eindverslag, dat bij de aanvraag voor subsidievaststelling gevoegd wordt, informatie bevatten waarmee kan worden vastgesteld of de subsidiabele activiteiten daadwerkelijk hebben plaatsgevonden, alsook of ze tot het gewenste eindresultaat hebben geleid. De te verschaffen informatie bestaat concreet uit een omschrijving van de projectresultaten van het cyberbeveiligingsinnovatieproject en op welke wijze het cyberbeveiligingsinnovatieproject heeft bijgedragen aan de doelen en deelgebieden.

3.3 Berekening van de administratieve lasten

Voor de berekening van de administratieve lasten is het volgende van belang:

De verwachting is dat per individuele subsidieaanvrager 24 uur aan de indiening van de subsidieaanvraag besteed wordt (bestaande uit onder meer de kennisname van de regeling, alsook verdere voorbereiding, het opstellen en indienen van de subsidieaanvraag. Uitgaande van 20 ingediende subsidieaanvragen zou het totale aantal uren voor het indienen van de subsidieaanvragen hiermee dan uitkomen op 480 uur.

De verwachting is dat de werkzaamheden ten behoeve van de aanvraag tot subsidievaststelling (zoals onder meer het opstellen van de eindrapportage en het indienen van de aanvraag tot subsidievaststelling) gemiddeld 6 uur in beslag zal nemen per aanvrager. Uitgaande van 13 gehonoreerde projecten zou het totale aantal uren voor het indienen van de aanvragen tot subsidievaststelling hiermee dan uitkomen op 78 uur.

De verwachting is dat de werkzaamheden ten behoeve van monitoring en evaluatie 2 uur per subsidieontvanger in beslag zal nemen. Uitgaande van 13 gehonoreerde projecten zou het totale aantal uren voor monitoring en evaluatie hiermee dan uitkomen op 26 uur.

Voor de berekening van de administratieve lasten is van belang dat uit het voorgaande volgt dat de tijdsbesteding (het totale aantal uren werk om aan de voormelde informatieverplichtingen te kunnen voldoen) naar verwachting uitkomt op 584 uur, waarvoor het toepasselijke uurtarief € 60 bedraagt. De totale administratieve lasten van alle projecten gezamenlijk komen dan uit op € 35.040. Dit is circa 3,77 procent van het subsidieplafond van € 930.000.



3.4 Beoordeling door Adviescollege toetsing regeldruk

Deze wijzigingsregeling is voorgelegd aan het Adviescollege toetsing regeldruk (ATR). Naar aanleiding hiervan is deze wijzigingsregeling niet geselecteerd voor formele advisering, omdat deze geen omvangrijke gevolgen voor de regeldruk heeft.

4. Uitvoering

De uitvoering van dit subsidie-instrumentarium is (namens NCC.NL gegeven) in handen van RVO.nl, onderdeel van het Ministerie van Economische Zaken en Klimaat. Deze subsidiemodule wordt uitvoerbaar en handhaafbaar geacht. Ook zal door RVO namens NCC.NL en/of door NCC.NL zelf voldaan worden aan de verplichtingen uit het Programma Digitaal Europa.

II. Artikelsgewijs

Artikel I (Regeling Nationale EZK- en LNV-subsidies)

Onderdelen A en B (artikelen 1.1 en 3.27.1)

In artikel 1.1 zijn de toepasselijke overkoepelende begripsbepalingen opgenomen voor de subsidiemodules (lees: titels en/of paragrafen) van de Regeling nationale EZK- en LNV-subsidies, waarin gebruik gemaakt wordt van bepaalde begrippen (uit dezelfde Europese steunkaders). Daarnaast zijn er in de diverse subsidiemodules (lees: titels) van de Regeling nationale EZK- en LNV-subsidies begripsbepalingen opgenomen, die uitsluitend betrekking hebben op de desbetreffende subsidiemodule. Dit laatste is bijvoorbeeld het geval in artikel 3.27.1 waarin onder meer de begripsbepalingen 'grote onderneming', 'organisatie-innovatie' en 'procesinnovatie' waren opgenomen. Omdat deze begrippen echter in het vervolg zowel in de subsidiemodule IPCEI (titel 3.27) als in de subsidiemodule Cyberbeveiligingsinnovatieprojecten (titel 4a.3.) gebruikt worden, zijn deze verplaatst van artikel 3.27.1 naar artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies.

Onderdeel C, Titel 4a.3. Cyberbeveiligingsinnovatieprojecten

Met dit onderdeel is een nieuwe titel 4.a3 opgenomen in de Regeling nationale EZK- en LNV-subsidies. Deze titel bevat de subsidiemodule Cyberbeveiligingsinnovatieprojecten.

Artikel 4a.3.1. Begripsbepalingen

In dit artikel zijn de begripsbepalingen opgenomen die van belang zijn voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten. Op deze begripsbepalingen wordt ingegaan in de artikelsgewijze toelichting op de artikelen 4a.3.2, 4a.3.3 en 4a.3.4.

Artikel 4a.3.2. Subsidieverstrekking

Dit artikel bevat een uitwerking van de reikwijdte van de doelstellingen, subsidiabele activiteiten en subsidieontvangers. Op de inhoud en achtergrond hiervan wordt in de volgende passages nader ingegaan.

Doelstelling van de subsidie (artikel 4a.3.2, eerste lid)

Op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten kan subsidie worden verstrekt aan een in Nederland gevestigde juridische entiteit voor het zelfstandig dan wel in een Nederlands of Europees samenwerkingsverband uitvoeren van een cyberbeveiligingsinnovatieproject. Dit project moet een bijdrage leveren aan de operationele doelen van specifieke doelstelling 3 uit het Programma Digitaal Europa zoals neergelegd in artikel 6, eerste lid, van verordening (EU) 2021/694. Zie voor de omschrijving van en achtergrond bij deze doelstellingen paragraaf 1.2 van het algemene deel van deze toelichting.

Verder is van belang dat de bijdrage aan deze operationele doelen nog meer geconcretiseerd is in, en moet plaatsvinden binnen, één of meer van de volgende deelgebieden, opgenomen in artikel 4a.3.2, eerste lid.

Het automatiseren van cyberbeveiliging oplossingen

Binnen dit deelgebied moeten de cyberbeveiligingsinnovatieprojecten betrekking hebben op het ontwikkelen van vernieuwende methoden of technieken en verspreiden van kennis over de automatisering van cyberbeveiligingsoplossingen. Het gaat hierbij om cyberbeveiligingsinnovatieprojecten op



het gebied van het automatisch voorspellen, opsporen en tegenhouden van dreigingen van cyberaanvallen, alsook het automatisch verspreiden van kennis en informatie over dreigingen van cyberaanvallen. Hierbij kan gedacht worden aan bijvoorbeeld het ontwikkelen van digitale replica's van fysieke systemen of processen (digital twins) of systemen en algoritmes om cyberaanvallen te voorspellen op basis van kunstmatige intelligentie, om vervolgens (automatisch) tot actie over te gaan. Via deze cyberbeveiligingsinfrastructuur kan een adequate preventie en antwoord geboden worden om de Nederlandse (vitale) digitale infrastructuur te beschermen tegen dreigingen, zoals malware, phishing en gegevensdiefstal. De snelheid, complexiteit of schaal waarop aanvallen kunnen gebeuren, maakt automatisering van cyberbeveiligingsoplossingen namelijk noodzakelijk.

Het behoud en de ontwikkeling van personeel

Binnen dit deelgebied moeten de cyberbeveiligingsinnovatieprojecten gericht zijn op het verbeteren en ontwikkelen van vernieuwende programma's betreffende het behoud en de ontwikkeling van personeel. Hierbij kan worden gedacht aan de ontwikkeling van een innovatieve opleidingsmodule, training of trainingsomgeving voor cyberbeveiliging, alsook het (door)ontwikkelen van specifieke competentieprofielen of een programma betreffende de uitwisseling van personeel en kennis tussen diverse organisaties (uit het bedrijfsleven en/of de overheid). Hiermee wordt beoogd een oplossing te bieden voor de huidige stagnatie van de ontwikkeling en implementatie van cyberbeveiligingsystemen, die het gevolg is van het huidige tekort aan geschikt personeel met de juiste expertise. Het lukt ondernemingen, overheden en andere organisaties namelijk onvoldoende om de cyberbeveiligingsvacatures in te vullen. Dit is het gevolg van een gebrek aan geschoold personeel, de hoge doorlooptijd van werknemers en het gebrek aan programma's die erop gericht zijn om geschikt personeel in de cyberbeveiligingssector te trainen en te behouden. De Cyberbeveiligingsinnovatieprojecten binnen dit deelgebied kunnen dan ook een bijdrage leveren aan de doorbreking van deze trend.

Het proportioneel, veilig en privacybeschermend delen van data

Binnen dit deelgebied moeten de cyberbeveiligingsinnovatieprojecten gericht zijn op het ontwikkelen van vernieuwende methoden of technieken voor proportioneel, veilig en privacybeschermend delen van data. Hierbij kan worden gedacht ofwel aan het ontwikkelen van methoden voor de ondersteuning van partijen in een samenwerkingsverband bij informatiedeling ofwel aan het ontwikkelen van technische oplossingen. De ontwikkeling van technische oplossingen kan bestaan uit het ontwikkelen van kunstmatig gegenereerde (synthetische) data voor het privacy-vriendelijk nabootsen van realistische situaties, alsook uit het ontwikkelen van crypto grafische technieken, zoals Secure Multi Party Computation (MPC) en kwantum-Safe (lees: Crypto grafische (QSC) oplossingen die bestand zijn tegen een crypto-analytische aanval van een kwantum computer). De Cyberbeveiligingsinnovatieprojecten binnen dit thema sluiten aan bij de groeiende behoefte van het delen van data tussen diverse partijen (in samenwerkingsverbanden), die vooral verband houden met de opkomst van kunstmatige intelligentie en Big Data. Vanwege de vereiste vertrouwelijkheid van de gegevens, alsook bestaande wet- en regelgeving op het gebied van privacy, is het belangrijk dat deze data proportioneel, veilig en privacybeschermend gedeeld wordt.

Het door ontwikkelen of opschalen van cyberbeveiligingsoplossingen

Binnen dit deelgebied moeten cyberbeveiligingsinnovatieprojecten gericht zijn op het toepassen van vernieuwende methoden en technieken in het belang van de nationale veiligheid of voor nieuwe marktsegmenten. Binnen dit deelgebied passen dan ook twee type projecten: cyberbeveiligingsinnovatieprojecten die opschaling mogelijk maken door hele specifieke (kleinschalige) cyberbeveiligingsoplossingen (lees: producten of diensten) door te ontwikkelen voor de bescherming van de gehele nationale veiligheid van Nederland. Het gaat hierbij om projecten die naar verwachting een grote impact of groot effect zullen hebben op de beveiliging van diverse Nederlandse ondernemingen en/of overheidsinstellingen. Hierbij kan worden gedacht aan de doorontwikkeling van een (kleinschalige) cyberbeveiligingsoplossing die nu slechts nog de veiligheid verbetert van bijvoorbeeld een Industrieel Controle Systeem, dat slechts op een select aantal plekken in Nederland wordt gebruikt. Deze cyberbeveiligingsoplossing zou doorontwikkeld kunnen worden voor een latere uitrol naar meer plaatsen in Nederland, om zo de beschikbaarheid, integriteit of vertrouwelijkheid van een vitaal proces of essentiële dienst voor de samenleving te waarborgen. cyberbeveiligingsinnovatieprojecten die opschaling mogelijk maken door het door ontwikkelen van (grootschalige) cyberbeveiligingsoplossingen, die al worden gebruikt voor de gehele nationale veiligheid, naar (meerdere specifieke kleinschalige) cyberbeveiligingsoplossingen, die bestemd zijn voor een bredere toepassing in een nieuw marktsegment. Voor cyberbeveiligingsoplossingen die een kleinschalig toepassingsgebied zullen hebben, is het lastig om financiering te vinden. De reden hiervoor is dat er een mogelijk gebrek is aan commerciële interesse. Toch is ondersteuning van de doorontwikkeling van deze cyberbeveiligingsoplossingen gewenst omdat deze van groot belang kunnen zijn voor de veiligheid van specifieke organisaties of de gehele nationale veiligheid.



Subsidiabele activiteiten (artikel 4a.3.2, tweede lid)

De subsidie is bestemd voor een cyberbeveiligingsinnovatieproject. Een cyberbeveiligingsinnovatieproject bevat een samenhangend geheel van activiteiten, bestaande uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie en/of proces- en organisatie-innovatie. Deze subsidiabele activiteiten worden verder afgebakend in artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies dat voor de invulling van deze activiteiten verwijst naar de begripsbepalingen van fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling, haalbaarheidsstudie, organisatie-innovatie en procesinnovatie zoals deze zijn opgenomen in artikel 2, onderdelen 84, 85, 86, 87, 96 en 97, van de algemene groepsvrijstellingsverordening. Daarnaast kan de meer specifieke inhoud van deze activiteiten afgeleid worden uit de voormelde deelgebiedomschrijvingen, opgenomen in de artikelsgewijze toelichting op artikel 4a.3.2, eerste lid. Hierbij is ook het onderscheid van belang tussen (1) niet-economische projectactiviteiten (die alleen uitgevoerd kunnen worden door een juridische entiteit die als onderzoeksorganisatie kwalificeert) en (2) economische projectactiviteiten (die uitgevoerd kunnen worden door een juridische entiteit die voor het uitvoeren van deze activiteiten als onderneming opereert).

Een juridische entiteit die als onderzoeksorganisatie kwalificeert, kan op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten voor subsidie in aanmerking komen voor het verrichten van niet-economische activiteiten. Uit artikel 4a.3.1 volgt dat een juridische entiteit als onderzoeksorganisatie kwalificeert in het geval deze beschouwd kan worden als 'een organisatie voor onderzoek en kennisverspreiding' als bedoeld in artikel 2, onderdeel 83, van de algemene groepsvrijstellingsverordening en paragraaf 1.3, onderdeel ee, van het O&O&I-steunkader. Deze onderzoeksorganisatie kan onder meer niet-economische activiteiten verrichten, die onafhankelijk uitgevoerd moeten worden met het oog op meer kennis en een beter inzicht. Het onafhankelijk uitvoeren van deze activiteiten is van belang om deze activiteiten als niet economisch te kunnen kwalificeren. Onder de subsidiemodule Cyberbeveiligingsinnovatieprojecten kunnen de niet-economische activiteiten van onderzoeksorganisaties bestaan uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling en/of een haalbaarheidsstudie, zolang deze onafhankelijk (los van wensen van ondernemingen en niet met een directe link met het aanbieden op een markt) verricht worden. De subsidiemodule Cyberbeveiligingsinnovatieprojecten sluit voor de reikwijdte van deze niet-economische activiteiten aan bij paragraaf 2.1.1 van het O&O&I-steunkader.

Een juridische entiteit die voor het uitvoeren van de projectactiviteiten als onderneming kwalificeert, kan op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten voor subsidie in aanmerking komen voor het verrichten van economische activiteiten. Een onderneming is op grond van artikel 1 van het Kaderbesluit iedere eenheid, ongeacht haar rechtsvorm of wijze van financiering, die een economische activiteit uitoefent. Voor zover voor het uitvoeren van economische activiteiten onder de subsidiemodule Cyberbeveiligingsinnovatieprojecten derhalve subsidie wordt verleend aan een juridische entiteit, zoals bv, nv, vereniging, stichting of andere entiteit, dan wordt deze voor het uitvoeren van deze economische activiteiten als onderneming aangemerkt. Hierbij is van belang dat een onderzoeksorganisatie onder de subsidiemodule Cyberbeveiligingsinnovatieprojecten ook (voor bepaalde activiteiten) als onderneming kan opereren (zie in dit verband ook de uitspraak van het Hof van Justitie van 13 oktober 2022, gevoegde zaken C-164/21 en C-318/21 over het begrip 'organisatie voor onderzoek en kennisverspreiding'). De economische activiteiten bestaan in dit geval uit industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie en/of proces- en organisatie-innovatie.

De subsidieverlening voor de voorgaande economische activiteiten wordt in beginsel gerechtvaardigd door artikelen 25 en 29 van de algemene groepsvrijstellingsverordening¹¹. In het geval er een verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, verstrekt is, kan de subsidieontvanger die economische activiteiten verricht echter ook gebruik maken van de mogelijkheid van (een hoger subsidiepercentage aan) subsidieverlening onder de algemene de-minimisverordening (zie artikel 4a.3.3). Wel moet er voldaan worden aan bepaalde randvoorwaarden uit artikel 1, eerste lid, onderdelen a, b en c, van de algemene de-minimisverordening, die zijn opgenomen in artikel 4a.3.2, derde lid, onderdeel d. Uit artikel 1, eerste lid, onderdelen a en b, van de algemene de-minimisverordening volgt dat de de-minimisverordening niet van toepassing is op de sectoren van de primaire productie van landbouwproducten, de visserij en de aquacultuur. Wat in de zin van de algemene de-minimisverordening onder landbouwproducten wordt verstaan, staat in bijlage I van het Verdrag betreffende de werking van de Europese Unie. Daarnaast is de algemene de-minimisverordening slechts van toepassing op de ondernemingen die zich bezighouden met de verwerking en de afzet van landbouwproducten en niet-landbouwproducten indien is voldaan aan de

¹¹ Verordening (EU) nr. 651/2014 van de Commissie van 17 juni 2014 waarbij bepaalde categorieën steun op grond van de artikelen 107 en 108 van het Verdrag met de interne markt verenigbaar worden verklaard (PbEU 2014, L 187).



voorwaarden die zijn opgenomen in artikel 1, eerste lid, onderdeel c, van de algemene de-minimisverordening. Indien de subsidieaanvragers actief zijn in de sectoren op het gebied van de primaire productie van landbouwproducten, de visserij en aquacultuur of de verwerking en afzet van landbouwproducten, en in dat laatste geval niet aan voormelde voorwaarden is voldaan, kan dus geen subsidie worden verleend. Ook kan geen subsidie worden verleend als de aan de algemene de-minimisverordening ontleende afwijzingsgrond uit artikel 4a.3.7, onderdeel g, van toepassing is of niet voldaan is aan de informatieverplichting uit artikel 4a.3.12, eerste lid, onderdeel d. Hierop wordt ingegaan in de artikelsgewijze toelichting op deze artikelen.

Subsidieontvangers (artikel 4a.3.2, derde lid)

De subsidieontvangers bestaan uit in Nederland gevestigde juridische entiteiten als bedoeld in artikel 2, onderdeel 2, van verordening (EU) 2021/694 (zie artikelen 4a.3.1 en 4a.3.2, derde lid)). Hiermee wordt invulling gegeven aan artikel 18, eerste lid, van verordening (EU) 2021/694 op grond waarvan alleen Europese cofinanciering (lees: subsidie) verstrekt mag worden aan (kort gezegd) juridische entiteiten die gevestigd zijn in een lidstaat van de Europese Unie of geassocieerd derde land (in dit geval dus een juridische entiteit die gevestigd is in Nederland). Ook moeten de juridische entiteiten aan de volgende kenmerken en voorwaarden voldoen.

Allereerst komen alleen voor subsidie in aanmerking de juridische entiteiten die (overeenkomstig artikel 18, derde lid, van verordening (EU) 2021/694)) niet kwalificeren als natuurlijke personen. Het zal dus in de regel gaan om in Nederland gevestigde privaatrechtelijke of publiekrechtelijke rechtspersonen. Een uitzondering hierop vormen provincies, gemeenten of openbaar lichamen als bedoeld in de Wet gemeenschappelijke regelingen, omdat er geen gebruik is gemaakt van de mogelijkheid uit artikel 3, tweede lid, van het Kaderbesluit om subsidie te kunnen verstrekken aan deze laatst genoemde overheidsorganen.

Ten tweede wordt alleen subsidie verstrekt aan een juridische entiteit die de subsidiabele activiteiten zelfstandig dan wel in een Nederlands of Europees samenwerkingsverband uitvoert. Voor de uitleg van de begrippen Nederlands en Europees samenwerkingsverband wordt verwezen naar de (hierna nog volgende afzonderlijke) artikelsgewijze toelichting op artikel 4a.3.2, derde lid, onderdeel b.

Ten derde wordt alleen subsidie verstrekt aan een juridische entiteit die gedurende het indienen van de aanvraag om subsidie, bedoeld in artikel 4a.3.12, en het uitvoeren van de activiteiten, bedoeld in het tweede lid, niet verbonden is in een groep met één of meer andere juridische entiteiten die niet zijn gevestigd in één van de landen als bedoeld in artikel 18 van verordening (EU) 2021/694. Hiermee moet voorkomen worden dat via bepaalde constructies (indirect) andere (niet gewenste) juridische entiteiten, die niet voldoen aan de voorwaarden van het Programma Digitaal Europa, ondersteund zouden worden door de subsidie en/of van de vergaarde kennis in het project zouden kunnen profiteren. Deze aan de subsidieontvanger verbonden voorwaarde wordt getoetst aan de hand van een ingevuld formulier bij de subsidieaanvraag, bedoeld in artikel 4a.3.12, tweede lid, onderdeel f.

Tot slot wordt alleen subsidie verstrekt aan een juridische entiteit die, voor zover deze een verklaring de-minimissteun als bedoeld in artikel 4a.3.12, eerste lid, onderdeel d, heeft overgelegd, ten behoeve van de uitvoering van de economische activiteiten, bedoeld in het tweede lid, onderdeel b, geen onderneming in stand houdt die actief is in (1°) de sector visserij en aquacultuur, (2°) de primaire productie van landbouwproducten of (3°) de sector verwerking en afzet van landbouwproducten in de gevallen, bedoeld in artikel 1, eerste lid, onderdeel c, van de algemene de-minimisverordening. Voor de achtergrond bij deze voorwaarden wordt verwezen naar de artikelsgewijze toelichting op artikel 4a.3.2, tweede lid.

Soorten samenwerkingsverbanden (artikel 4a.3.2, derde lid, onderdeel b)

Uit artikel 4a.3.2, derde lid, onderdeel b, volgt dat er alleen subsidie wordt verstrekt aan een juridische entiteit die de subsidiabele activiteiten zelfstandig dan wel in een Nederlands of Europees samenwerkingsverband uitvoert. Deze samenwerkingsverbanden moeten voldoen aan de volgende voorwaarden.

Het Europese samenwerkingsverband, waar de Nederlandse juridische entiteit onderdeel van kan uitmaken, moet voldoen aan de voorwaarden van het Programma Digitaal Europa, en dan met name de voorwaarden die op grond van artikel 18 van verordening (EU) 2021/694 gesteld worden aan juridische entiteiten om deel te nemen aan dit programma. Behoudens de uitzonderingen, genoemd in artikel 18, tweede, derde en vierde lid, van verordening (EU) 2021/694, gaat het in de regel om (a) juridische entiteiten, niet-zijnde natuurlijke personen, die zijn gevestigd in (i) een lidstaat of een met een lidstaat verbonden land of gebied overzee; of (ii) een overeenkomstig de artikelen 10 en 12 van verordening (EU) 2021/694 met het programma Digitaal Europa geassocieerd derde land of b) elke



krachtens het recht van de Europese Unie opgerichte andere juridische entiteit en elke internationale organisatie van Europees belang.

Verder kan de in Nederland gevestigde (privaatrechtelijke of publiekrechtelijke) juridische entiteit het cyberbeveiligingsinnovatieproject ook uitvoeren binnen een samenwerkingsverband (zoals gedefinieerd in artikel 1 van het Kaderbesluit) van in Nederland gevestigde onafhankelijke juridische entiteiten (hierna: het (Nederlandse) samenwerkingsverband). Bij het cyberbeveiligingsinnovatieproject kan bijvoorbeeld door ondernemingen, onderzoeksorganisaties samengewerkt worden. Alle deelnemers aan het (Nederlandse) samenwerkingsverband worden beschouwd als individuele subsidieaanvragers. In de praktijk kan ook een penvoerder namens (alle deelnemers uit) het Nederlandse samenwerkingsverband de aanvraag om subsidieverlening indienen. Dit is bepaald in artikel 20 van het Kaderbesluit. Het is de bedoeling dat de penvoerder zelf ook subsidiabele activiteiten verricht. De beschikking tot subsidieverlening wordt verzonden aan de penvoerder, maar de subsidie zal uiteindelijk verleend en betaald worden aan de subsidieontvanger (individuele deelnemer uit het samenwerkingsverband) die de desbetreffende subsidiabele activiteiten uitvoert.

Artikel 4a.3.3. Hoogte subsidie

In dit artikel is voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten aangegeven welke steunintensiteiten en welk maximum subsidiebedrag voor de subsidiabele kosten gehanteerd worden.

Steunintensiteit voor niet-economische activiteiten (artikel 4a.3.3, eerste lid, onderdeel a)

Voor niet-economische activiteiten, bestaande uit fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling en/of een haalbaarheidsstudie, wordt op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten een steunintensiteit van 100 procent van de subsidiabele kosten gehanteerd, omdat hiermee een maximale stimulans gegeven kan worden voor de uitvoering van deze gewenste niet-economische activiteiten. Op deze activiteiten zijn de steunkaders, met eventuele beperking van de steunintensiteit niet van toepassing. Voor wat al dan niet onder niet-economisch fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling of een haalbaarheidsstudie van een onderzoeksorganisatie wordt verstaan, wordt aangesloten bij het O&O&I-steunkader.

Steunintensiteit voor economische activiteiten via Algemene de-minimis-verordening (artikel 4a.3.3, eerste lid, onderdeel b)

Voor economische activiteiten, bestaande uit industrieel onderzoek, experimentele ontwikkeling, een haalbaarheidsstudie of proces- en organisatie-innovatie, door een juridische entiteit die kwalificeert als een onderneming en die een verklaring de-minimissteun heeft overgelegd, bedraagt de steunintensiteit 100% van de subsidiabele kosten. Hiervoor is gekozen om ook in dit geval een maximale stimulans te geven aan de voormelde subsidiabele economische activiteiten. Hierbij geldt echter wel de beperking dat het totale bedrag aan de-minimissteun bij een Cyberbeveiligingsinnovatieproject voor een subsidieontvanger (die dit project zelfstandig of in een samenwerkingsverband) uitvoert niet meer kan bedragen dan het maximumbedrag, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening (het zogenaamde de-minimisplafond van € 200.000 over een periode van drie belastingjaren). Dit plafond ziet op alle vormen van steun die op grond van de desbetreffende de-minimisverordening verleend kan worden. Op grond van artikel 22, eerste lid, onderdeel b, subonderdeel 1°, van het Kaderbesluit zal een aanvraag om subsidie worden afgewezen indien (op voorhand duidelijk is) dat subsidietoekenning zou leiden tot overschrijding van het de-minimisplafond.

Steunintensiteit voor economische activiteiten via algemene groepsvrijstellingsverordening (artikel 4a.3.3, eerste lid, onderdeel c)

Voor economische activiteiten door een juridische entiteit die kwalificeert als een onderneming en die geen verklaring de-minimissteun heeft overgelegd, worden de volgende subsidiepercentages gehanteerd voor grote, middelgrote en kleine ondernemingen¹².

¹² Voor de afbakening van het begrip 'grote onderneming' aan de ene kant en de begrippen 'middelgrote en kleine onderneming' aan de andere kant wordt in artikel 1 van de Regeling Nationale EZK- en LNV-subsidies verwezen naar artikel 2, onderdeel 24, van de algemene groepsvrijstellingsverordening respectievelijk bijlage I van de algemene groepsvrijstellingsverordening. Hieruit volgt dat grote ondernemingen bestaan uit ondernemingen die niet voldoen aan de vastgestelde criteria in bijlage I van de algemene groepsvrijstellingsverordening. Ondernemingen die wel aan deze criteria voldoen, kwalificeren namelijk als middelgrote of kleine onderneming. Een middelgrote onderneming is een onderneming waarbinnen minder dan 250 personen werkzaam zijn en waarvan de jaaromzet 50 miljoen EUR en/of het jaarlijkse balanstotaal 43 miljoen EUR niet overschrijdt. Een kleine onderneming is een onderneming waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt. De wijze waarop het aantal werknemers en de omzet berekend moeten worden, volgt ook uit voormelde bijlage.



Voor de onderzoeksactiviteiten bedragen de basispercentages van de steunintensiteit voor industrieel onderzoek 50 procent van de subsidiabele kosten, voor experimentele ontwikkeling 25 procent van de subsidiabele kosten en voor een haalbaarheidsstudie 50 procent van de subsidiabele kosten. Daarbij is gebruik gemaakt van de mogelijkheid van artikel 25 van de algemene groepsvrijstellingsverordening om voor kleine of middelgrote ondernemingen de voormelde basispercentages voor industrieel onderzoek, experimentele ontwikkeling en haalbaarheidsstudies met 10 procentpunten op te hogen. Voor deze ophoging is van belang dat de aanvrager dus een middelgrote of kleine onderneming moet zijn en dat de bij de subsidiabele activiteit horende subsidiabele kosten ook worden gemaakt en betaald door deze middelgrote respectievelijk kleine onderneming. De subsidie wordt namelijk uitsluitend verstrekt voor de kosten die een subsidieontvanger zelf maakt voor het uitvoeren van zijn subsidiabele activiteiten (inclusief de kosten die de subsidieontvanger maakt voor de aanschaf van producten of inhuur van een derde). De noodzakelijke gegevens over de bedrijfsgrootte moeten bij de subsidieaanvraag worden overgelegd (zie de toelichting op artikel 4a.3.12, eerste lid, onderdeel f, betreffende informatieverplichtingen). Opgemerkt wordt dat vanwege de praktische uitvoerbaarheid geen gebruik is gemaakt van de mogelijkheid van artikel 25 van de algemene groepsvrijstellingsverordening om de subsidiepercentages nog eens extra op te hogen voor kleine ondernemingen (met nog eens 10 procent) en bij daadwerkelijke samenwerking of kennisverspreiding (met nog eens 15%). Voor proces- en organisatie-innovatie bedraagt de steunintensiteit 15 procent van de subsidiabele kosten voor proces- en organisatie-innovatie door een grote onderneming en 50 procent van de subsidiabele kosten voor proces- en organisatie-innovatie door een kleine of middelgrote onderneming.

Maximum (subsidie)bedrag (artikel 4a.3.3, derde lid)

In artikel 4a.3.3, derde lid, wordt bepaald dat de subsidie per cyberbeveiligingsinnovatieproject ten hoogste € 75.000 kan bedragen. Er is voor dit maximum gekozen om ervoor te zorgen dat in voldoende mate geschikte (omvangrijke) projecten ondersteund kunnen worden, zonder dat bijvoorbeeld één project het subsidieplafond grotendeels of geheel kan gebruiken. Ook wordt met dit maximum-subsidiebedrag gebleven binnen de zogenaamde drempelbedragen die op grond van artikel 4, eerste lid van de algemene groepsvrijstellingsverordening van toepassing zijn op bepaalde economische activiteiten die vallen onder artikelen 25 en 29 van de algemene groepsvrijstellingsverordening (zie paragraaf 2 van het algemene deel van deze toelichting). Vanwege de eenduidigheid wordt voor alle subsidiabele activiteiten (voor zowel de niet-economische als economische subsidiabele activiteiten) in deze subsidiemodule hetzelfde maximumsubsidiebedrag gehanteerd.

Artikel 4a.3.4. Subsidiabele kosten

In dit artikel is (in aanvulling op artikel 10 Kaderbesluit) bepaald wat de subsidiabele kosten zijn. Op grond van artikel 10 Kaderbesluit is het uitgangspunt dat alleen de redelijk gemaakte kosten die direct verbonden zijn met de uitvoering van een activiteit in aanmerking kunnen komen voor subsidie. In het vervolg van artikel 10 Kaderbesluit wordt dit uitgangspunt verder uitgewerkt via specifieke regels die betrekking hebben op de vraag welke kosten wel en niet in aanmerking komen voor subsidie. Hiermee wordt gewaarborgd dat het verband tussen de kosten en de subsidiabele activiteit (direct en duidelijk) aanwezig is.

In aanvulling op voorgaande bepaling is voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten in artikel 4a.3.4 opgesomd wat voor categorieën van kosten voor subsidie in aanmerking komen. Het betreft hier de kosten die vermeld staan in artikelen 25 en 29 van de algemene groepsvrijstellingsverordening. Deze artikelen bevatten kostensoorten die voor subsidie in aanmerking komen in het geval de subsidieverlening betrekking heeft op economische activiteiten. Voor de kosten voor niet-economische activiteiten zijn niet direct bepalingen in een Europees staatssteunkader opgenomen. Vanwege de eenduidigheid is er evenwel voor gekozen om zowel voor niet-economische als economische activiteiten in deze subsidiemodule aan te sluiten bij de begrenzing van de kostensoorten zoals opgenomen in artikelen 25 en 29 van de algemene groepsvrijstellingsverordening.

Voor de berekeningsmethoden voor het bepalen van de subsidiabele kosten wordt verwezen naar artikelen 11 tot en met 14 van het Kaderbesluit, die de subsidieontvanger de keuze geeft om de subsidiabele kosten te berekenen met behulp van (a) de integrale kostensystematiek (IKS), (b) de loonkosten plus vaste-opslag-systematiek of (c) de vaste-uurtarief-systematiek). Daarnaast moet bij economische activiteiten ook voldaan worden aan de berekeningsmethode uit het toepasselijke Europese steunkader (in dit geval de algemene groepsvrijstellingsverordening) zoals deze zijn neergelegd in artikel 1.7 van de Regeling nationale EZK- en LNV-subsidies.

Artikel 4a.3.5. Verdeling van het subsidieplafond

Dit artikel bepaalt op welke wijze het subsidieplafond verdeeld wordt. Dat zal gebeuren op volgorde



van binnenkomst van de aanvragen (waarbij alleen volledige subsidieaanvragen direct verdeeld kunnen worden en onvolledige subsidieaanvragen pas als deze adequaat zijn aangevuld). Door deze wijze van verdeling wordt beoogd de procedure van subsidieverstrekking op een zo efficiënt mogelijke wijze plaats te laten vinden. Om de subsidieaanvragers in staat te stellen snel met de uitvoering van de cyberbeveiligingsinnovatieprojecten te starten en om snel duidelijkheid te geven over de financiering, is gekozen voor directe behandeling bij binnenkomst en directe subsidieverlening bij gebleken geschiktheid van het cyberbeveiligingsinnovatieproject. Indien op de datum dat het subsidieplafond wordt bereikt meer dan één volledige subsidieaanvraag ontvangen wordt, wordt de onderlinge rangschikking van de volledige subsidieaanvragen vastgesteld door middel van loting op grond van artikel 27 van het Kaderbesluit.

Artikel 4a.3.6. Start- en realisatietermijn

In dit artikel is bepaald dat met de uitvoering van een op grond van deze subsidiemodule gesubsidieerd cyberbeveiligingsinnovatieproject moet worden gestart voor 1 februari 2024. Op deze wijze wordt gewaarborgd dat het desbetreffende project spoedig van start zal gaan. Het gaat immers om een subsidiemodule die onderdeel is van het Programma Digitaal Europa waarbij het van belang is dat projecten snel kunnen starten en binnen afzienbare termijn tot tastbare resultaten leiden die bijdragen aan cyberbeveiliging. Ook kan alleen Europese cofinanciering verstrekt worden in het geval projecten spoedig van start gaan en afgerond worden.

Aanvullend hierop is de realisatietermijn vastgesteld op zes maanden. Dit betekent dat het desbetreffende cyberbeveiligingsinnovatieproject zes maanden na de start hiervan gerealiseerd moet zijn. Indien uit het bij de subsidieaanvraag aangeleverde projectplan blijkt dat het cyberbeveiligingsinnovatieproject niet binnen deze termijn gerealiseerd zou kunnen worden, wordt de subsidie afgewezen op grond van artikel 23, aanhef en onderdeel b, van het Kaderbesluit. Er is voor deze termijn gekozen, omdat de beleidsmatige wens en verwachting is dat een cyberbeveiligingsinnovatieproject binnen de gestelde realisatietermijn kan worden afgerond.

Van belang is nog wel dat artikel 37, derde lid, van het Kaderbesluit in geval van vertraging van de uitvoering van de activiteiten of het essentieel wijzigen hiervan aan de Minister van Economische Zaken en Klimaat de bevoegdheid geeft om ontheffing te verlenen van de verplichting om de activiteiten overeenkomstig het projectplan van de subsidieontvanger uit te voeren. Gelet op de deadlines betreffende de Europese cofinanciering, is de verwachting echter dat een verzoek tot verlenging van de realisatietermijn niet altijd gehonoreerd zal worden.

Artikel 4a.3.7. Afwijzingsgronden

Dit artikel bevat de afwijzingsgronden die, in aanvulling op de afwijzingsgronden uit artikel 22 en 23 van het Kaderbesluit, van toepassing zijn.

Allereerst wordt de subsidieaanvraag afgewezen indien het cyberbeveiligingsinnovatieproject naar verwachting in onvoldoende mate bijdraagt aan de doelen en de deelgebieden, bedoeld in artikel 4a.3.2, eerste lid. Voor een beschrijving van de wijze waarop aan de doelen en deelgebieden voldaan kan worden, wordt verwezen naar de artikelsgewijze toelichting op artikel 4a.3.2, eerste lid. De doelstellingen en deelgebieden waaraan een bijdrage wordt geleverd, zou moeten volgen uit het projectplan van het cyberbeveiligingsinnovatieproject, bedoeld in artikel 4a.3.12, tweede lid, onderdeel a.

Ten tweede wordt de subsidieaanvraag afgewezen indien de kwaliteit van het projectplan van het cyberbeveiligingsinnovatieproject, bedoeld in artikel 4a.3.12, tweede lid, onderdeel a, onvoldoende is. Een aanvraag voor een cyberbeveiligingsinnovatieproject zal dus worden afgewezen indien er sprake is van een inadequate uitwerking van de onderzoeksmethode en inhoudelijke aanpak, alsook in het geval dat het projectplan een inadequate beschrijving geeft van de inhoudelijke aanpak, de uit te voeren activiteiten, meetbare indicatoren en go/no go momenten, de te gebruiken middelen en de beoogde resultaten. Ook zal een aanvraag voor een cyberbeveiligingsinnovatieproject worden afgewezen in het geval de kwaliteit onvoldoende is van de inventarisatie en analyse van de risico's die een succesvolle uitvoering van het cyberbeveiligingsinnovatieproject kunnen bedreigen en wat voor mitigerende maatregelen hiervoor genomen (kunnen) worden.

Ten derde wordt de subsidieaanvraag afgewezen indien de subsidiabele kosten onevenredig zijn ten opzichte van de beoogde resultaten van het cyberbeveiligingsinnovatieproject. De subsidieaanvraag wordt afgewezen in het geval de beschikbare financiële middelen onvoldoende effectief of efficiënt worden ingezet met het oog op de te bereiken doelen van het cyberbeveiligingsinnovatieproject. De financiële middelen betreffen zowel de gevraagde subsidie als andere financiële middelen waarmee het cyberbeveiligingsinnovatieproject gefinancierd wordt. Om te voorkomen dat er onnodig veel kosten opgevoerd worden, wordt bij de beoordeling van de subsidieaanvraag meegewogen welke impact het desbetreffende projectvoorstel kan hebben op de doelstellingen gerelateerd aan de totale



subsidiabele kosten die opgevoerd worden. Subsidieaanvragen voor projecten die een geringe impact zullen hebben ten opzichte van de totale opgevoerde kosten zullen dan ook worden afgewezen. De kostenopbouw en verdeling hiervan volgt uit de bij de subsidieaanvraag aan te leveren projectbegroting (zie artikel 4a.3.12, tweede lid, onderdeel b).

Ten vierde wordt de subsidieaanvraag afgewezen indien de voor de uitvoering van het cyberbeveiligingsinnovatieproject benodigde competenties in onvoldoende mate aanwezig zijn binnen de subsidieaanvrager die het cyberbeveiligingsinnovatieproject uitvoert. Bij deze afwijzingsgrond wordt de geschiktheid van de subsidieaanvrager getoetst aan de aanwezigheid van de voor de uitvoering van het cyberbeveiligingsinnovatieproject benodigde competenties. De geschiktheid van de subsidieaanvrager zou onder meer kunnen blijken uit een beknopte beschrijving van de competenties van de bij de uitvoering van het cyberbeveiligingsinnovatieproject betrokken organisaties of personen (zie artikel 4a.3.12, tweede lid, onderdeel c).

Ten vijfde wordt de subsidieaanvraag afgewezen indien de verwachte impact van het cyberbeveiligingsinnovatieproject op de markt en maatschappij onvoldoende is. Deze afwijzingsgrond is in twee situaties van toepassing:

Deze afwijzingsgrond is van toepassing in het geval de verwachte toepassingsmogelijkheden en slaagkans van de met het project te ontwikkelen innovatie of innovaties onvoldoende zijn voor de Nederlandse en internationale markt. Waar bij de voorgaande afwijzingsgronden de nadruk ligt op de input, de activiteiten en de output van het project, gaat het bij deze afwijzingsgrond om de gevolgen en de verwachte impact. Een goede onderbouwing, waar mogelijk kwantitatief, van de verwachtingen op dit punt is voor de beoordeling van deze afwijzingsgrond belangrijk, de aannames en inschattingen dienen expliciet gemaakt te worden. Zo moet in het projectplan onderbouwd worden op welke soort cyberbeveiligingstransitie (in de markt) het project betrekking heeft, en hoe de bijdrage aan de desbetreffende transitie tot stand komt. Dit kan blijken uit de toepassingsmogelijkheden en de slaagkans op de markt. Het gaat hierbij dus om de toepassingsmogelijkheden van de ontwikkelde producten of diensten op het gebied van cyberbeveiliging binnen de doelen op één of meer van de deelgebieden, bedoeld in artikel 4a.3.2, eerste lid. Om de toepassing van deze afwijzingsgrond te voorkomen, is concreet van belang (a) om goed te onderbouwen in welke sectoren/marktsegmenten behoefte is aan de voorgestelde oplossingen (producten, processen en/of diensten) en (b) een adequate omschrijving en onderbouwing te geven van de visie op het implementatietraject, door inzicht te geven in de vervolgstappen die bij een positief resultaat gezet zullen worden in de verdere ontwikkeling en marketing van de voorgestelde oplossingen en door wie, zo mogelijk tot aan introductie op de markt. Dit kan beoordeeld worden aan de hand van de beknopte beschrijving, bedoeld in artikel 4a.3.12, tweede lid, onderdeel d, betreffende de strategie en ontwikkelprioriteiten van de subsidieaanvrager en op welke termijn het te ontwikkelen product of dienst de markt naar verwachting zal bereiken en welke impact het daar zal hebben.

Verder wordt voormelde afwijzingsgrond ook toegepast in het geval er naar verwachting onvoldoende draagvlak bestaat voor het cyberbeveiligingsinnovatieproject binnen in Nederland gevestigde ondernemingen, maatschappelijke organisaties of overheden. Het gaat hierbij onder meer om het versterken van de onderlinge samenwerking met externe partijen en het betrekken van stakeholders die voor het project van belang zijn. Zo kan bijvoorbeeld gekeken worden naar de brede betrokkenheid van (grote, middelgrote en kleine) ondernemingen, onderzoeksorganisaties en mogelijke andere verschillende soorten (maatschappelijke) partijen uit de hele keten van de desbetreffende sector of aanverwante sectoren bij het project. Hiermee wordt bedoeld op de partijen die belang hebben bij de uitvoering van het project (stakeholders), maar zelf het onderzoeksprogramma niet uitvoeren, zoals bepaalde producenten, ontwikkelaars, afnemers en eindgebruikers die onder meer kunnen bestaan uit energiemaatschappijen, hightech-ondernemingen, milieuorganisaties, landbouwondernemingen, land- en tuinbouworganisaties, onderwijs- en kennisinstellingen, visserijondernemingen en zorginstellingen.

Ten zesde wordt de subsidieaanvraag afgewezen indien de verwachte impact van het cyberbeveiligingsinnovatieproject op in Nederland gevestigde middelgrote of kleine ondernemingen onvoldoende is. De impact is onvoldoende in het geval dat (1°) er niet ten minste één middelgrote of kleine onderneming deelneemt aan het cyberbeveiligingsinnovatieproject of (2°) er geen toepassingsmogelijkheden zijn van de ontwikkelde producten of diensten binnen de organisatie van middelgrote of kleine ondernemingen. Hiermee wordt invulling gegeven aan de focus op projecten van of ten behoeve van kleine of middelgrote ondernemingen, opgenomen in de operationele doelstelling uit artikel 6, eerste lid, onderdeel c, van verordening (EU) 2021/694 betreffende het Programma Digitaal Europa. Deze operationele doelstelling sluit aan bij overweging 8 van verordening (EU) 2021/887, waaruit volgt dat kleine en middelgrote ondernemingen cruciale stakeholders zijn voor cyberbeveiliging en dat het EKC en de NCC's vooral aan deze kleine en middelgrote ondernemingen steun moeten verlenen (door de toegang tot kennis te vergemakkelijken en door toegang op maat tot onderzoeks- en ontwikkelingsresultaten te bieden). Hierdoor zouden kleine en middelgrote ondernemingen zich voldoende kunnen beveiligen en mogelijk kunnen concurreren en bijdragen tot de leidende positie



van de Europese Unie op het gebied van cyberbeveiliging.

Ten zevende wordt de subsidieaanvraag afgewezen indien de te verlenen subsidie minder dan € 25.000 per subsidieaanvrager zou bedragen. Op deze wijze wordt ervoor gezorgd dat de bijdragen van de subsidieaanvrager die het project zelfstandig of in een samenwerkingsverband uitvoert voldoende substantieel is bij een subsidieverlening van (ten hoogste) € 75.000 per cyberinnovatieproject (zie artikel 4a.3.3, tweede lid). Het is dus niet mogelijk om voor de uitvoering van een project aan 10 subsidieaanvragers € 7.500 aan subsidie te verlenen, maar slechts aan drie (of minder) subsidieaanvragers te minste € 25.000.

Tot slot is er een afwijzingsgrond opgenomen die ervoor zorgt dat de subsidieverstrekking aan bepaalde subsidieaanvragers wordt gerechtvaardigd door de algemene de-minimisverordening. Er is geëxpliciteerd dat, voor zover de subsidieaanvraag is ingediend door een subsidieaanvrager als bedoeld in artikel 4a.3.2, derde lid, geen subsidie wordt verleend voor activiteiten die direct verband houden met: (1°) de omvang van de uitvoer naar andere lidstaten van de Europese Unie of derde landen, (2°) het oprichten en exploiteren van een distributienet ten behoeve van de uitvoer of (3°) andere lopende uitgaven direct verband houdend met activiteiten op het gebied van uitvoer. Dit is in lijn met artikel 1, eerste lid, onderdeel d, van de algemene de-minimisverordening.

Artikel 4a.3.9. Verplichtingen betreffende niet-economische activiteiten door onderzoeksorganisaties

Dit artikel heeft betrekking op de verplichtingen voor onderzoeksorganisaties die niet-economische onderzoeksactiviteiten uitvoeren.

Afgescheiden boekhouding van niet-economische activiteiten (artikel 4a.3.9, eerste lid)

Bij het zelfstandig of in een samenwerkingsverband uitvoeren van niet-economische activiteiten is het van belang dat er een duidelijk onderscheid gemaakt kan worden tussen economische en niet-economische activiteiten. Om te kunnen beoordelen welke activiteiten niet-economisch van aard zijn, dient de onderzoeksorganisatie een gescheiden boekhouding bij te houden tussen economische- en niet-economische activiteiten, waarin ook de niet-economische activiteiten van het cyberbeveiligingsinnovatieproject kunnen worden onderscheiden (zie artikel 4a.3.9, eerste lid). Hiermee wordt invulling gegeven aan paragraaf 2.1.1, onderdeel 16, van het O&O&I-steunkader, waarin wordt bepaald dat niet-economische en economische activiteiten en de kosten, financiering en inkomsten ervan duidelijk kunnen worden onderscheiden, zodat kruissubsidiëring van de economische activiteiten (met de subsidie voor niet-economische activiteiten) wordt vermeden. Het bewijs van een correcte toerekening van kosten, financiering en inkomsten kan worden geleverd door (het overleggen van) de financiële jaarrekeningen van de betrokken onderzoeksorganisatie.

Het verrichten van niet-economische activiteiten in een samenwerkingsverband (artikel 4a.3.9, tweede tot en met vierde lid)

Voor het uitvoeren van onderzoeksactiviteiten in een samenwerkingsverband is het volgende van belang.

Allereerst moet er op grond van artikel 4a.3.9, tweede lid, aanhef en onderdeel b, sprake zijn van daadwerkelijke samenwerking met een onderneming, waarvoor in artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies onder meer wordt verwezen naar de begripsbepaling in paragraaf 1.3, onderdeel h, van het O&O&I-steunkader. Op grond hiervan bestaat daadwerkelijke samenwerking uit een samenwerking tussen ten minste twee onafhankelijke partijen om kennis of technologie uit te wisselen of om een gemeenschappelijke doelstelling op basis van een taakverdeling te bereiken. Hierbij dienen de partijen samen de omvang van het samenwerkingsproject te bepalen, bij te dragen aan de tenuitvoerlegging ervan, en het risico en de resultaten ervan te delen. Een of meer partijen zouden de volledige kosten van het cyberbeveiligingsinnovatieproject kunnen dragen en zodoende de andere partijen bevrijden van de aan het cyberbeveiligingsinnovatieproject verbonden financiële risico's. Vanzelfsprekend worden contractonderzoek en het verrichten van onderzoeksdiensten niet als vormen van samenwerking beschouwd. Artikel 4a.3.9 bewerkstelligt voorts dat, in het geval er sprake is van fundamenteel onderzoek, industrieel onderzoek, experimentele ontwikkeling of een haalbaarheidsstudie door een onderzoeksorganisatie, de voordelen die een onderzoeksorganisatie geniet niet als indirecte staatssteun doorgegeven worden aan een onderneming waarmee de onderzoeksorganisatie in samenwerking activiteiten verricht. Aan welke voorwaarden bij daadwerkelijke samenwerking voldaan moet worden is verder uitgewerkt in paragraaf 2.2.2 van het O&O&I-steunkader, waarvan randnummer 28 bepaalt dat de voorwaarden van een samenwerkingsproject, met name wat betreft de bijdrage in de kosten ervan, het delen in de risico's en uitkomsten ervan, de verspreiding van de resultaten, de toegang tot en de regels voor de toewijzing van intellectuele-eigendomsrechten vóór de

aanvang van het cyberbeveiligingsinnovatieproject moeten zijn overeengekomen. Naast de verplichting tot daadwerkelijke samenwerking, opgenomen in artikel 4a.3.9, tweede lid, onderdeel b, is in artikel 4a.3.9, tweede lid, onderdeel a, dan ook een aanvullende verplichting voor de subsidieaanvragers opgenomen om voorafgaand aan de start van het cyberbeveiligingsinnovatieproject een samenwerkingsovereenkomst te sluiten waarin voormelde afspraken neergelegd zijn.

Ten tweede wordt met artikel 4a.3.9, tweede lid, onderdeel c, verzekerd dat een onderzoeksorganisatie en een onderneming ten opzichte van elkaar handelen als normale marktpartijen. Deze voorwaarden zijn in lijn met de vereisten uit paragraaf 2.2.2, randnummers 29 en 30, van het O&O&I-steunkader. Wanneer cyberbeveiligingsinnovatieprojecten gezamenlijk door ondernemingen en onderzoeksorganisaties worden uitgevoerd, is de Europese Commissie volgens randnummer 29 van het O&O&I-steunkader van oordeel dat er met de gunstige samenwerkingsvoorwaarden via die entiteiten geen indirecte staatssteun aan de deelnemende ondernemingen wordt verleend indien aan één van de volgende voorwaarden is voldaan:

(a) de deelnemende ondernemingen dragen de volledige kosten van de activiteiten van het cyberbeveiligingsinnovatieproject (zie voor deze voorwaarde artikel 4a.3.9, tweede lid, onderdeel c, subonderdeel 1°;

(b) de resultaten van de samenwerking die geen intellectuele-eigendomsrechten opleveren kunnen breed worden verspreid en alle intellectuele-eigendomsrechten die de activiteiten van de onderzoeksorganisatie opleveren worden volledig toegekend aan die entiteiten (zie voor deze voorwaarde artikel 4a.3.9, tweede lid, onderdeel c, subonderdeel 2°;

(c) uit het cyberbeveiligingsinnovatieproject ontstane intellectuele-eigendomsrechten, alsmede daarmee verband houdende toegangsrechten, worden aan de verschillende samenwerkende partners toegekend op een wijze die een passende afspiegeling is van hun werkpakketten, bijdragen en respectieve belangen. Bij voormelde toegangsrechten, opgenomen in artikel 4a.3.9, tweede lid, onderdeel c, subonderdeel 3°, kan gedacht worden aan gebruiksrechten en licenties;

(d) de onderzoeksorganisaties ontvangen een vergoeding die gelijkwaardig is aan de marktprijs voor de intellectuele-eigendomsrechten die uit hun activiteiten ontstaan en worden overgedragen aan de deelnemende ondernemingen of waartoe de deelnemende ondernemingen toegangsrechten kregen toegewezen. Het absolute bedrag van – financiële en niet financiële – bijdragen van de deelnemende ondernemingen in de kosten van de activiteiten van de onderzoeksorganisatie die de betrokken intellectuele-eigendomsrechten hebben opgeleverd, kan op die vergoeding in mindering worden gebracht (zie voor deze voorwaarde artikel 4a.3.9, tweede lid, onderdeel c, subonderdeel 4°, en het derde lid. Voorts bewerkstelligt een onderzoeksorganisatie dat de voormelde vergoeding overeenstemt met de marktprijs, door één van de alternatieven te kiezen die opgesomd staan en uitgewerkt zijn in artikel 4a.3.9, vierde lid, onderdelen a tot en met d, en vijfde lid. Hiermee wordt invulling gegeven aan randnummer 30 van het O&O&I-steunkader.

Indien geen van de vorenstaande voorwaarden is vervuld, zal de volledige waarde van de bijdrage van de onderzoeksorganisatie aan het cyberbeveiligingsinnovatieproject (overeenkomstig randnummer 31 van het O&O&I-steunkader) worden beschouwd als een (economisch) voordeel voor de samenwerkende ondernemingen, waarvoor de regels inzake staatssteun gelden. In dat geval zal gekeken moeten worden of de (indirecte) subsidieverlening aan deze ondernemingen past binnen de grenzen van het dan toepasselijke staatssteunkader (artikel 25 van de algemene groepsvrijstellingsverordening).

Buiten toepassing verklaring artikel 1.9 van de Regeling nationale EZK- en LNV-subsidies (artikel 4a.3.9, vijfde lid)

Tot slot is van belang dat in artikel 1.9 van de Regeling nationale EZK- en LNV-subsidies een soortgelijke (minder verregaande) bepaling als in artikel 4a.3.9 is opgenomen. Om te voorkomen dat er een verschil in interpretatie tussen artikelen 1.9 en 4a.3.9 zou ontstaan, is artikel 1.9 niet van toepassing verklaard op deze subsidiemodule.

Artikel 4a.3.10. Verplichtingen betreffende proces- en organisatie-innovatie door een grote onderneming

Op grond van de subsidiemodule Cyberbeveiligingsinnovatieprojecten wordt onder meer subsidie verstrekt voor activiteiten betreffende proces- en organisatie-innovatie door (een juridische entiteit die kwalificeert als) een onderneming. De verlening van deze subsidie is staatssteun die gerechtvaardigd wordt door artikel 29 van de algemene groepsvrijstellingsverordening. Hierbij is van belang dat artikel 29, tweede lid, van de algemene groepsvrijstellingsverordening aanvullende voorwaarden bevat voor het geval de subsidiabele activiteiten verricht worden door een grote onderneming als bedoeld in artikel 2, onderdeel 24, van de algemene groepsvrijstellingsverordening (zie artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies). Om te waarborgen dat ook aan deze randvoorwaarden voldaan wordt, is in artikel 4a.3.10 nog een aantal aanvullende verplichtingen voor deze onderneming opgenomen. Hierin wordt bepaald dat voormelde projectactiviteiten door de grote onderneming



moeten worden uitgevoerd in daadwerkelijke samenwerking met middelgrote en kleine ondernemingen, die ten minste 30% van de totale subsidiabele kosten dragen.

Artikel 4a.3.11. Verplichtingen betreffende voorlichting

Voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten bevat dit artikel verplichtingen om bepaalde kennis opgedaan tijdens de uitvoering van de activiteiten openbaar te verspreiden.

De subsidieontvanger moet de niet bedrijfsgevoelige kennis en informatie die met het gesubsidieerde cyberbeveiligingsinnovatieproject wordt opgedaan na afloop van het project openbaar bekendmaken via (a) daarvoor geschikte conferenties, publicaties, open access-repositories dan wel gratis of opensource-software als bedoeld in artikel 25, zesde lid, onderdeel b, subonderdeel II, van de algemene groepsvrijstellingsverordening en (b) voor zover van toepassing, via een op verzoek van en naar het oordeel van de Minister opgesteld (1°) kwalitatief voldoende verslag, dat wordt verstrekt met gebruikmaking van een middel dat door de Minister beschikbaar wordt gesteld of (2°) adequaat voorlichtingsmateriaal, dat wordt gepresenteerd tijdens een geschikte conferentie. Deze verplichting geldt gedurende twee jaar na de datum van de beschikking tot subsidievaststelling.

Met deze voorlichting kan bijgedragen worden aan de versnelling van de verdere brede implementatie van de in het gesubsidieerde cyberinnovatieproject opgedane kennis (binnen de relevante sectoren). Ook kunnen door deze voorlichting de kosten voor navolgers verlaagd worden (die gemaakt worden bij toekomstige cyberbeveiligingsinnovatieprojecten of investeringsprojecten), omdat geleerd kan worden van de afgeronde gesubsidieerde cyberbeveiligingsinnovatieprojecten.

Artikel 4a.3.12. Informatieverplichtingen

In dit artikel zijn informatieverplichtingen opgenomen ten aanzien van de gegevens die de subsidieaanvraag moet bevatten of waarvan deze vergezeld dient te gaan.

Informatieverstrekking in de subsidieaanvraag (artikel 4a.3.12, eerste lid)

Het eerste lid van dit artikel maakt duidelijk welke informatie in een subsidieaanvraag opgenomen moet worden.

Allereerst betreft het hier onder meer de minimale informatievereisten over de subsidieaanvrager en het project, die nodig zijn om de aanvraag te kunnen behandelen. Deze vereisten sluiten (grotendeels) aan bij de wijze waarop andere (vergelijkbare) subsidiemodules in de Regeling nationale EZK- en LNV-subsidies zijn vormgegeven.

Ook wordt in dit artikellid bepaald welke informatie verstrekt moet worden in het geval de subsidie staatssteun bevat die wordt gerechtvaardigd door de algemene de-minimisverordening of algemene groepsvrijstellingsverordening. Het betreft hier gegevens die van belang zijn om aan de monitoringsverplichting te voldoen die elke lidstaat van de Europese Unie richting de Europese Commissie heeft. Het gaat hierbij om de volgende informatie.

In het geval de subsidie (voor economische activiteiten) staatsteun bevat die door de algemene de-minimisverordening wordt gerechtvaardigd, is het van belang dat een verklaring de-minimissteun verstrekt wordt. In deze verklaring moet de subsidieaanvrager bevestigen dat subsidieverlening niet zal leiden tot een overschrijding van het de-minimisplafond, bedoeld in artikel 3, tweede lid, van de algemene de-minimisverordening (zie voor de beschrijving van het begrip verklaring de-minimissteun ook artikel 1.1 van de Regeling nationale EZK- en LNV-subsidies). Daarom moet een subsidieaanvraag een verklaring de-minimissteun bevatten, indien de subsidieaanvrager aanspraak wil maken op het percentage aan subsidie, bedoeld in artikel 4a.3.3, eerste lid, onderdeel b.

In het geval de subsidie (voor economische activiteiten) staatsteun bevat die door artikel 25 en 29 van de algemene groepsvrijstellingsverordening wordt gerechtvaardigd (en de subsidieaanvrager dus aanspraak wil maken op de subsidiepercentages, bedoeld in artikel 4a.3.3, eerste lid, onderdeel c), moeten de basisgegevens, bedoeld in artikel 6, tweede lid, van de algemene groepsvrijstellingsverordening, worden verstrekt. Daarnaast moeten er ook gegevens verstrekt worden over de grootte van de onderneming van de subsidieaanvrager, indien de subsidieaanvrager aanvullend aanspraak wil maken op een verhoogd percentage aan subsidie voor een kleine of middelgrote onderneming als bedoeld in artikel 4a.3.3, tweede lid, die gebaseerd zijn op artikel 25 van de algemene groepsvrijstellingsverordening.

Informatieverstrekking in de bijlage bij de subsidieaanvraag (artikel 4a.3.12, tweede lid)

In het tweede lid wordt bepaald dat de subsidieaanvraag vergezeld dient te gaan van bepaalde bescheiden.



Allereerst moet de subsidieaanvraag op grond van artikel 4a.3.12, tweede lid, onderdelen a en b, vergezeld gaan van (a) een projectplan met daarin een projectomschrijving van doelen, deelgebieden en de activiteiten, bedoeld in artikel 4a.3.2, eerste en tweede lid, van het cyberbeveiligingsinnovatieproject of (b) een projectbegroting waarin per projectfase en deelnemer een omschrijving wordt gegeven van (1°) de omvang van de gevraagde subsidie en (2°) de totale subsidiabele kosten van het cyberbeveiligingsinnovatieproject en op welke activiteiten als bedoeld in artikel 4a.3.2, tweede lid, deze kosten betrekking hebben. Met deze informatie kan een adequaat beeld verkregen worden van de doelstellingen en werkzaamheden binnen het cyberbeveiligingsinnovatieproject en aanverwante kosten, zodat onder meer getoetst kan worden aan de minimale eisen betreffende de doelstellingen, kwaliteit van het projectplan en evenredigheid van de kosten, opgenomen in de afwijzingsgronden, bedoeld in artikel 4a.3.7, onderdelen a, b en c.

Ten tweede moet op grond van artikel 4a.3.12, tweede lid, onderdeel c, ook een beknopte beschrijving verschaft worden van de competenties van de bij de uitvoering van het cyberbeveiligingsinnovatieproject betrokken organisaties of personen. De informatie over deze organisaties en/of personen is van belang om de geschiktheid van de subsidieaanvrager(s) te kunnen beoordelen, waaraan onder meer getoetst wordt via de minimale eisen op dit gebied, opgenomen in de afwijzingsgrond, bedoeld in artikel 4a.3.7, onderdeel c.

Ten derde moet op grond van artikel 4a.3.12, tweede lid, onderdeel d, een beknopte beschrijving verschaft worden van de strategie en ontwikkelprioriteiten van de subsidieaanvrager en op welke termijn het te ontwikkelen product of dienst de markt naar verwachting zal bereiken en welke impact het daar zal hebben. Hiermee kan de verwachte impact van het cyberbeveiligingsinnovatieproject op de markt en maatschappij getoetst worden, opgenomen in de afwijzingsgrond, bedoeld in artikel 4a.3.7, onderdeel e.

Ten vierde moet op grond van artikel 4a.3.12, tweede lid, onderdeel e, een samenwerkingsovereenkomst verschaft worden. Hiermee wordt getoetst of voldaan zal worden aan de verplichtingen uit het O&O&I-steunkader, opgenomen in artikel 4a.3.9, tweede lid, onderdeel a.

Ten vijfde moet op grond van artikel 4a.3.12, tweede lid, onderdeel f, ook een ingevuld formulier verschaft worden waaruit volgt dat de subsidieaanvrager niet in een groep verbonden is met één of meer andere juridische entiteiten die niet zijn gevestigd in één van de landen als bedoeld in artikel 18 van verordening (EU) 2021/694. Er moet namelijk voorkomen worden dat via bepaalde constructies (indirect) toch andere (niet gewenste) juridische entiteiten ondersteund zouden worden door de subsidie en zouden kunnen profiteren van de vergaarde kennis in het project. Deze verklaring kan hierbij behulpzaam zijn en draagt bij aan de beoordeling van de voorwaarde uit artikel 4a.3.2, derde lid, onderdeel c. Het in te vullen modelformulier wordt door de Minister beschikbaar gesteld.

Tot slot is van belang dat op grond van artikel 19, eerste lid, van het Kaderbesluit een aanvraag om subsidie moet worden ingediend met gebruikmaking van een middel dat beschikbaar wordt gesteld. Dit middel zal aan het begin van de openstellingsperiode beschikbaar worden gesteld via www.rvo.nl. De bij de aanvraag in te dienen documenten kunnen (behoudens de voormelde Nederlandse samenvatting van het project) ook in de Engelse taal worden aangeleverd, gelet op het Europese proces.

Artikel 4a.3.13. Aanvraag subsidievaststelling

Voor de Regeling nationale EZK- en LNV-subsidies zijn de verplichtingen inzake subsidievaststelling opgenomen in artikel 50 van het Kaderbesluit. Er is evenwel voor gekozen om deze verplichtingen in dit artikel nader in te vullen. Dit artikel bevat een opsomming van de informatie die in ieder geval opgenomen moet worden in het eindverslag, bedoeld in artikel 50, tweede lid, onderdeel a, van het Kaderbesluit, dat bij de aanvraag voor subsidievaststelling wordt ingediend. Deze onderdelen dienen ervoor om te bezien of de subsidiabele activiteiten daadwerkelijk hebben plaatsgevonden, alsook of de subsidiabele activiteiten tot het gewenste eindresultaat hebben geleid. Het eindverslag dient in ieder geval de volgende zaken te bevatten: (a) een omschrijving van de projectresultaten van het cyberbeveiligingsinnovatieproject en (b) op welke wijze het cyberbeveiligingsinnovatieproject heeft bijgedragen aan de doelen en deelgebieden, bedoeld in artikel 4a.3.2, eerste lid.

De verdere effecten van de subsidie kunnen (later ook nog) via een evaluatie getoetst worden. Op grond van artikel 41 van het Kaderbesluit dient de subsidieontvanger namelijk gedurende vijf jaar na de datum van de beschikking tot subsidievaststelling medewerking te verlenen aan een evaluatie van de doeltreffendheid en de effecten van de aan hem verleende subsidie, voor zover medewerking redelijkerwijs van hem kan worden verlangd.



Artikel 4a.3.14. Staatssteun

De subsidie, bedoeld in artikel 4a.3.2, eerste lid, met uitzondering van de subsidie voor niet-economische activiteiten, bedoeld in artikel 4a.3.2, tweede lid, onderdeel a, bevat staatsteun en wordt gerechtvaardigd door: (a) de algemene de-minimisverordening, indien de subsidieaanvrager aanspraak wil maken op het percentage aan subsidie, bedoeld in artikel 4a.3.3, eerste lid, onderdeel b, (b) de artikelen 25 en 29 van de algemene groepsvrijstellingsverordening, indien de subsidieaanvrager aanspraak wil maken op de percentages aan subsidie als bedoeld in artikel 4a.3.3, eerste lid, onderdeel c, of tweede lid. Voor een uitgebreidere toelichting op de staatssteunaspecten wordt verwezen naar paragraaf 2 van het algemene deel van deze toelichting.

Artikel 4a.3.15. Vervaltermijn

In artikel 4.10, tweede lid, van de Comptabiliteitswet 2016 is bepaald dat subsidieregelingen een vervaltermijn van maximaal vijf jaren bevatten. Artikel 4a.3.15 geeft invulling aan voormelde bepaling. Dit artikel bepaalt namelijk voor de onderhavige subsidiemodule wat de vervaldatum is. Deze subsidiemodule vervalt na vijf jaar, met ingang van 1 oktober 2028. Te zijner tijd zal bezien worden of het wenselijk is deze titel te verlengen. De (mogelijke) ontwerpregeling inzake een dergelijke verlenging zal, overeenkomstig artikel 4.10, zevende lid, van de Comptabiliteitswet 2016, aan de Tweede Kamer worden overgelegd.

Artikel II (Regeling openstelling EZK- en LNV-subsidies 2023)

In de tabel van artikel 1 van de Regeling openstelling EZK- en LNV-subsidies 2023 is aangegeven in welke periode de diverse subsidiemodules van de Regeling nationale EZK- en LNV-subsidies zijn opengesteld en wat het subsidieplafond bedraagt. Hieraan is ook de openstelling van de subsidiemodule Cyberbeveiligingsinnovatieprojecten toegevoegd.

Voor de subsidiemodule Cyberbeveiligingsinnovatieprojecten loopt de openstellingsperiode van 2 oktober 2023 om 9.00 uur tot en met 2 november 2023 om 17.00 uur. Het subsidieplafond wordt vastgesteld op € 930.000.

Artikel III (inwerkingtreding)

Deze regeling treedt in werking met ingang van 1 oktober 2023. Met de datum van inwerkingtreding wordt aangesloten bij de systematiek van de vaste verandermomenten, inhoudende dat ministeriële regelingen met ingang van de eerste dag van elk kwartaal in werking treden. Wel wordt afgeweken van de regel dat ministeriële regelingen minimaal twee maanden voor inwerkingtreding bekend worden gemaakt. Dat kan in dit geval worden gerechtvaardigd, omdat de doelgroep gebaat is bij spoedige inwerkingtreding van deze regeling. Op deze wijze wordt de doelgroep de mogelijkheid geboden om spoedig subsidieaanvragen in te dienen. Vasthouden aan de systematiek van de vaste verandermomenten en bekendmakingstermijn zou hebben betekend dat subsidieaanvragen pas vanaf het eerstvolgende vaste verandermoment op 1 januari 2024 ingediend zouden kunnen worden. Ook heeft de doelgroep voldoende tijd om aanvragen in te dienen en voor te bereiden, omdat de subsidiemodule opengesteld wordt vanaf 2 oktober 2023 tot en met 2 november 2023.

*De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens*