STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 6765
17 februari
2026

Regeling van de Minister van Economische Zaken van 8 februari 2026, nr. WJZ/ 89969880 tot wijziging van de Uitvoeringsregeling cyberbeveiligingsverordening in verband met de uitvoering van uitvoeringsverordening (EU) 2024/482

De Minister van Economische Zaken,

Gelet op uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) en de artikelen 7 en 8 van de Uitvoeringswet cyberbeveiligingsverordening;

Besluit:

ARTIKEL I

De Uitvoeringsregeling cyberbeveiligingsverordening wordt als volgt gewijzigd:

A

In artikel 1 worden in de alfabetische volgorde de volgende begripsbepalingen ingevoegd:

AVA_VAN-niveau: AVA_VAN-niveau als bedoeld in artikel 2, onderdeel 8, van uitvoeringsverordening (EU) 2024/482;
certificeringsinstantie: certificeringsinstantie als bedoeld in artikel 2, onderdeel 12, van uitvoeringsverordening (EU) 2024/482;
EUCC-certificaat: EUCC-certificaat als bedoeld in artikel 2, onderdeel 9, van uitvoeringsverordening (EU) 2024/482;
ITSEF: ITSEF als bedoeld in artikel 2, onderdeel 7, van uitvoeringsverordening (EU) 2024/482;
technisch domein: technisch domein als bedoeld in artikel 2, onderdeel 13, van uitvoeringsverordening (EU) 2024/482;
uitvoeringsverordening (EU) 2024/482: uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC);
uitvoeringsverordening (EU) 2024/3143: uitvoeringsverordening (EU) 2024/3143 van de Commissie van 18 december 2024 tot vaststelling van de omstandigheden, vormen en procedures van aanmeldingen overeenkomstig artikel 61, lid 5, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie;.

B

Artikel 2 komt te luiden:

Artikel 2

Als voorschriften als bedoeld in artikel 8 van de wet worden aangewezen:
a. de artikelen 53, tweede en derde lid, 55, 56, vierde, zevende, achtste en negende lid, 63 en 64 van de cyberbeveiligingsverordening;
b. de voorschriften in uitvoeringsverordening (EU) 2024/482 met betrekking tot de verplichtingen van certificeringsinstanties, ITSEF's, of aanvragers of houders van een EUCC-certificaat.

C

Na artikel 2 worden drie artikelen ingevoegd, luidende:

Artikel 2a

1. Het is een certificeringsinstantie verboden zonder de autorisatie, bedoeld in artikel 21 van uitvoeringsverordening (EU) 2024/482, een EUCC-certificaat op zekerheidsniveau 'hoog' af te geven.

2. Een certificeringsinstantie dient een aanvraag voor autorisatie elektronisch in bij Onze Minister, met gebruikmaking van een door Onze Minister beschikbaar gesteld middel en voorzien van de op het aanvraagformulier vermelde bescheiden, tenzij technische belemmeringen aan de zijde van Onze Minister dit tijdelijk onmogelijk maken.

3. Een aanvraag als bedoeld in het tweede lid omvat:
   a. informatie over de aanvrager, genoemd in punt 3 van de bijlage bij uitvoeringsverordening (EU) 2024/3143;
   b. een bewijsstuk, dan wel bewijsstukken, waaruit blijkt dat de certificeringsinstantie die de autorisatie aanvraagt, voldoet aan de vereisten van artikel 60, eerste lid, en van de bijlage bij de cyberbeveiligingsverordening, en
   c. een bewijsstuk, dan wel bewijsstukken, waaruit blijkt dat de certificeringsinstantie die autorisatie aanvraagt, voldoet aan de vereisten van artikel 21, eerste lid, van uitvoeringsverordening (EU) 2024/482.

Artikel 2b

1. Een ITSEF dient een aanvraag voor autorisatie, bedoeld in artikel 22 van uitvoeringsverordening (EU) 2024/482, elektronisch in bij Onze Minister, met gebruikmaking van een door Onze Minister beschikbaar gesteld middel, tenzij technische belemmeringen aan de zijde van Onze Minister dit tijdelijk onmogelijk maken.

2. Een aanvraag als bedoeld in het eerste lid omvat:
   a. informatie over de aanvrager, genoemd in punt 3 van de bijlage bij uitvoeringsverordening (EU) 2024/3143;
   b. een bewijsstuk, dan wel bewijsstukken, waaruit blijkt dat de ITSEF die de autorisatie aanvraagt, voldoet aan de vereisten van artikel 60, eerste lid, en van de bijlage bij de cyberbeveiligingsverordening, en
   c. een bewijsstuk, dan wel bewijsstukken, waaruit blijkt dat de certificeringsinstantie die autorisatie aanvraagt, voldoet aan de vereisten van artikel 22, eerste lid, van uitvoeringsverordening (EU) 2024/482.

Artikel 2c

Een certificeringsinstantie die op grond van uitvoeringsverordening (EU) 2024/482 bevoegd is om een certificaat af te geven, en een ITSEF die op grond van uitvoeringsverordening (EU) 2024/482 bevoegd is om een evaluatie uit te voeren, verstrekken ten behoeve van de kennisgeving, bedoeld in artikel 23, respectievelijk artikel 24 van uitvoeringsverordening (EU) 2024/482, aan Onze Minister de volgende informatie middels een door Onze Minister beschikbaar gesteld middel:

a. de naam en het adres van de certificeringsinstantie respectievelijk de ITSEF;
b. het zekerheidsniveau of de zekerheidsniveaus waarvoor de certificeringsinstantie bevoegd is om EUCC-certificaten af te geven, respectievelijk waarvoor de ITSEF bevoegd is om een evaluatie uit te voeren;
c. de datum van de accreditatie;
d. het referentienummer van de accreditatie;
e. het toepassingsgebied en de geldigheidsduur van de accreditatie;
f. het adres van, de locatie van en de link naar de relevante website van de nationale accreditatie-instantie;
g. indien van toepassing:
   i. de datum van de autorisatie;
   ii. het referentienummer van de autorisatie;
   iii. de geldigheidsduur van de autorisatie;
   iv. het toepassingsgebied van de autorisatie, met inbegrip van het hoogste AVA_VAN-niveau en, indien van toepassing, de betreffende technische domeinen.

ARTIKEL II

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

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

's-Gravenhage, 8 februari 2026

De Minister van Economische Zaken,
V.P.G. Karremans

TOELICHTING

Algemene deel

1. Doel en aanleiding

Met deze regeling wordt uitvoering gegeven aan uitvoeringsverordening (EU) 2024/482. Met deze uitvoeringsverordening heeft de Europese Commissie de eerste Europese cyberbeveiligingscertificeringsregeling op basis van verordening (EU) 2019/881 (de cyberbeveiligingsverordening) – de European Common Criteria based certification scheme (EUCC) – vastgesteld. De EUCC vormt het Europese kader voor cyberbeveiligingscertificering van ICT-producten en bevat nadere bepalingen over de voorwaarden, procedures en technische eisen voor certificering.

Deze regeling voorziet in de nationale uitvoeringsbepalingen die nodig zijn om de EUCC in Nederland toe te passen. De regeling bepaalt op welke wijze conformiteitsbeoordelingsinstanties een autorisatie kunnen aanvragen en welke informatie zij daarbij moeten verstrekken. Daarnaast bevat de regeling de bepalingen die nodig zijn om de naleving van de verplichtingen uit de EUCC te kunnen handhaven.

Cyberbeveiligingsverordening

Op 28 juni 2021 is de Europese cyberbeveiligingsverordening[1] volledig van kracht geworden. Deze verordening introduceerde een Europees kader voor cyberbeveiligingscertificering. De op grond van de cyberbeveiligingsverordening vastgestelde Europese cyberbeveiligingscertificeringsregelingen vormen de basis voor de uitgifte van cyberbeveiligingscertificaten voor ICT-producten, -diensten en -processen. Deze certificaten worden in een EU-lidstaat afgegeven en worden in alle lidstaten erkend. Deelname aan de cyberbeveiligingscertificeringsregelingen is op dit moment vrijwillig.

EUCC

In 2024 is de EUCC als eerste Europese cyberbeveiligingscertificeringsregeling vastgesteld. Deze regeling is gebaseerd op het beproefde SOG-IS[2] Common Criteria-kader voor cyberbeveiligingscertificering, dat al in 17 EU-lidstaten werd gebruikt.

De EUCC richt zich op de op cyberbeveiligingscertificering van ICT-producten. Chips in bijvoorbeeld bankpassen of paspoorten, routers, besturingssystemen zoals Windows, Android of iOS, slimme meters, wachtwoordmanagers en chips in mobiele telefoons kunnen nu gecertificeerd worden volgens de eisen van de EUCC. Door certificering krijgen bedrijven, organisaties en consumenten meer zekerheid over de veiligheid van ICT-producten, omdat die door een onafhankelijke conformiteitsbeoordelingsinstantie uitgebreid zijn getest op cyberveiligheidseisen. De EUCC voorziet in twee zekerheidsniveaus – substantieel en hoog, afhankelijk van het risiconiveau dat verband houdt met het beoogde gebruik van het product.

De EUCC bevat criteria zowel voor te certificeren producten als voor het toezicht op conformiteitbeoordelingsinstanties en certificaathouders. Onderdeel van de criteria voor certificaathouders is het openbaar maken van kwetsbaarheidsinformatie, en consumentenondersteuning, zoals uitgebreide patchbeheerdiensten voor de gecertificeerde producten.

Conformiteitsbeoordelingsinstanties moeten overeenkomstig de EUCC worden geaccrediteerd en, indien van toepassing, geautoriseerd voor het uitvoeren van werkzaamheden onder de EUCC. In het kader van deze accreditatie- en autorisatieprocedures wordt onder meer beoordeeld of de desbetreffende partijen voldoende competent zijn en voldoen aan de eisen om de cyberveiligheid van ICT-producten te kunnen beoordelen overeenkomstig de eisen van de EUCC.

Fabrikanten en leveranciers wereldwijd kunnen een cyberbeveiligingscertificaat aanvragen in Nederland. Indien het ICT-product voldoet aan de eisen van de EUCC, kan een certificerende instantie hen een cyberbeveiligingscertificaat verstrekken. Dit certificaat wordt in de gehele Europese Unie erkend.

---

[1] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PbEU 2019, L151).

[2] SOG-IS staat voor Senior Officials Group – Information Systems Security.
Het is een Europese samenwerkingsovereenkomst gericht op de wederzijdse erkenning van IT-beveiligingsevaluaties, met name op basis van de Common Criteria (CC).

Voor de uitgifte van cyberbeveiligingscertificaten met het zekerheidsniveau hoog geldt op grond van de Uitvoeringswet cyberbeveiligingsverordening (hierna: de wet) een goedkeuringsprocedure voor het onderzoeksplan en het onderzoeksrapport. Bij het goedkeuringsmodel is in Nederland gekozen voor een systeem van stapsgewijze goedkeuring door de nationale cyberbeveiligingscertificeringsautoriteit (NCCA). De Rijksinspectie Digitale Infrastructuur (RDI) is op grond van de Uitvoeringswet cyberbeveiligingsverordening aangewezen als de NCCA in Nederland en heeft de taak om toezicht te houden op de cyberbeveiligingsverordening en uitvoering te geven aan de Europese cybersecuritycertificeringsregelingen in Nederland, waaronder de EUCC. De conformiteitsbeoordelingsinstantie meldt eerst bij de NCCA dat zij een certificeringstraject start. Vervolgens legt zij het onderzoeksplan ter goedkeuring voor aan de NCCA. Tot slot legt de conformiteitsbeoordelingsinstantie het onderzoeksrapport en het bijbehorende Europese cyberbeveiligingscertificaat dat zij voornemens is af te geven, ter goedkeuring voor aan de NCCA. Na goedkeuring door de NCCA kan de conformiteitsbeoordelingsinstantie het Europese cyberbeveiligingscertificaat afgeven.

Nadat het certificaat is afgegeven, houdt de NCCA toezicht op de naleving door de certificaathouder van de eisen die aan het certificaat zijn verbonden. Deze eisen omvatten onder meer het monitoren van kwetsbaarheden in het product, het verstrekken van updates om deze kwetsbaarheden te verhelpen, en het aanbieden van het product voor hercertificering bij wijzigingen. Hoewel de EUCC geen specifieke termijn voor deze processen voorschrijft, geldt als uitgangspunt dat de doorlooptijd, met behoud van kwaliteit, zo kort mogelijk is.

2. Inhoud

2.1 Conformiteitsbeoordelingsinstanties: certificeringsinstantie en ITSEF

Onder de cyberbeveiligingsverordening wordt de overkoepelende term conformiteitsbeoordelingsinstantie gehanteerd. Deze term verwijst naar elke instantie die belast is met het uitvoeren van conformiteitsbeoordelingsactiviteiten, waaronder certificering en evaluatie. Conformiteitsbeoordelingsinstantie betreft een brede verzamelterm die binnen de EUCC nader is gespecificeerd:
– Een certificeringsinstantie (CI) is verantwoordelijk voor het formeel afgeven van het cyberbeveiligingscertificaat op basis van de uitgevoerde evaluatie door een testende instantie.
– Een Information Technology Security Evaluation Facility (ITSEF) is een gespecialiseerde testinstantie die de technische beveiligingsevaluaties uitvoert van ICT-producten.

Hoewel beide typen organisaties functioneel onder het bredere begrip ‘conformiteitsbeoordelingsinstantie’ vallen, worden zij binnen de EUCC afzonderlijk benoemd vanwege hun onderscheiden rollen in het certificeringsproces.

2.2. Autorisatie certificeringsinstanties en ITSEF’s

Certificeringsinstanties en ITSEF’s moeten geaccrediteerd zijn om werkzaamheden in het kader van de EUCC te mogen uitvoeren. Voor certificeringswerkzaamheden op het zekerheidsniveau hoog geldt daarnaast dat zowel de certificeringsinstanties als de ITSEF’s formeel worden toegelaten (geautoriseerd) tot het certificeringsstelsel door de NCCA. Deze autorisatie is vereist omdat de EUCC aanvullende toelatingseisen stelt voor dit hogere zekerheidsniveau. Deze eisen hebben onder meer betrekking op competenties, expertise en maatregelen ter bescherming van product testresultaten en productontwerp.

Uit de cyberbeveiligingsverordening volgt dat de NCCA uitsluitend certificerende instanties mag autoriseren die in Nederland zijn gevestigd. Voor ITSEF’s geldt dat deze binnen de Europese Unie gevestigd moeten zijn.

Deze regeling stelt de procedure vast voor het aanvragen van de autorisatie en bepaalt welke gegevens bij de aanvraag moeten worden overgelegd. De aanvraag voor autorisatie wordt elektronisch ingediend via het door de Minister beschikbaar gestelde RDI-portaal. Indien elektronische indiening tijdelijk niet mogelijk is vanwege technische belemmeringen aan de zijde van de RDI, kunnen de aanvragen op papier worden ingediend.

Om aan te tonen dat voldaan wordt aan de eisen beschreven in de artikelen 21 en 22 van de uitvoeringsverordening (EU) 2024/3143), moet informatie aangeleverd worden waaronder:
– naam, adresgegevens en accreditatie zoals genoemd in punt 3 van de bijlage waar in bovengenoemde artikelen naar wordt verwezen;
– rechtspersoonlijkheid, onafhankelijkheid en onpartijdigheid van de aanvrager van de certificatie zoals genoemd in de bijlage bij de cyberbeveiligingsverordening;
– de wijze van beveiliging van verwerkte informatie, de competenties en expertise.

De NCCA beoordeelt de ingediende informatie en daar waar er informatie ontbreekt worden aanvul-

lende onderzoeken uitgevoerd. De bevinding wordt vastgelegd in een autorisatierapport en bevestigd in een formeel besluit aan de aanvrager.

2.3 Aanmelding conformiteitsbeoordelingsinstanties bij de Europese Commissie

Op grond van artikel 61, eerste lid, van de cyberbeveiligingsverordening heeft de NCCA de verplichting om de geaccrediteerde en, voor zover het het zekerheidsniveau hoog betreft, geautoriseerde conformiteitsbeoordelingsinstanties aan te melden bij de Europese Commissie. De procedure van de aanmelding is uitgewerkt in uitvoeringsverordening (EU) 2024/3143 van de Commissie van 18 december 2024 tot vaststelling van de omstandigheden, vormen en procedures van aanmeldingen overeenkomstig artikel 61, lid 5, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie. De bijlage bij de bedoelde uitvoeringsverordening bevat de informatie die voor de aanmelding nodig is.

Deze regeling bevat de verplichting voor de certificeringsinstanties en ITSEF's om de in de genoemde uitvoeringsverordening bedoelde gegevens ten behoeve van de aanmelding aan te leveren. De NCCA doet vervolgens een melding middels het Europese systeem NANDO voor de aanmelding van Notified Bodies.
Uit de cyberbeveiligingsverordening volgt dat de NCCA uitsluitend certificerende instanties mag notificeren die in Nederland zijn gevestigd. Voor ITSEF's geldt dat deze binnen de Europese Unie gevestigd moeten zijn.

2.4 Aanwijzing voorschriften

Op basis van artikel 8 van de wet worden met deze regeling bepalingen uit uitvoeringsverordening (EU) 2024/482 aangewezen zodat bestuursrechtelijke handhaving mogelijk is.

3. Regeldruk

ATR heeft de regeling niet geselecteerd voor een formeel advies, omdat de regeling geen omvangrijke gevolgen heeft voor de regeldruk.

De onderhavige regeling raakt twee type partijen, te weten: certificeringsinstanties (CI's) en gespecialiseerde testinstanties (ITSEF's) die de verplichtingen moeten naleven.

Aangezien het een concurrerende markt betreft is de verwachting dat het aantal certificeringsinstanties in Nederland beperkt blijft tot drie. Er zijn geen signalen dat de markt in de toekomst zal veranderen. Voor gespecialiseerde testinstanties geldt hetzelfde en is de verwachting dat het aantal partijen beperkt zal blijven tot zeven.

De genoemde uitvoeringsverordeningen betreffen een nadere uitwerking van de cyberbeveiligingsverordening, waarbij de volgende aspecten van belang zijn voor deze regeling:

a. *De verplichting tot accreditatie* wordt in de EUCC nader uitgewerkt met de criteria die de nationale accreditatieinstelling hanteert bij de accreditatie. Een conformiteitsbeoordelingsinstantie vraagt eenmalig bij de nationale accreditatieinstelling accreditatie aan om ICT-producten onder de EUCC te mogen certificeren.
b. *De verplichting tot autorisatie* is middels de EUCC nader uitgewerkt en toegespitst op organisaties die werkzaamheden willen uitvoeren op zekerheidsniveau hoog. Het verzamelen en indienen van de benodigde informatie voor enkel de autorisatie vergt van de ITSEF of CI een tijdsbesteding van naar schatting 16 tot 40 uur, afhankelijk van de volwassenheid van de organisatie. De tijdsbesteding voor een eventueel onderzoek ter plaatse zijn afhankelijk van de omvang van de organisatie en ligt naar schatting tussen de circa 16 tot 32 uur per locatie.
   Initieel dienen partijen eenmalig geaccrediteerd en, waar noodzakelijk voor zekerheidsniveau hoog, geautoriseerd en door de NCCA genotificeerd te worden. De accreditatie en autorisatie hebben een geldigheid van maximaal 5 jaar en dienen jaarlijks onderhouden te worden door de nationale accreditatieinstelling en de NCCA. Als er geen significante wijzigingen zijn geweest is de werklast verwaarloosbaar. Als er wel significante wijzigingen hebben plaatsgevonden, dient er mogelijk een herbeoordeling te worden uitgevoerd. De werklast hiervoor is vergelijkbaar met de initiële accreditatie en autorisatie.
   De NCCA kan bij de autorisatie gebruik maken van de beoordelingsrapporten van de betrokken nationale accreditatieinstellingen. De NCCA en de Nederlandse nationale accreditatieinstelling (Raad voor Accreditatie) maken bij hun accreditatie en autorisatie werkzaamheden gebruik van

elkaars expertise, zoals vastgelegd in een samenwerkingsovereenkomst.[3] Dit leidt tot een verminderde werklast voor de aanvragende partijen.

c. De *verplichting tot notificeren* door een NCCA is nader gespecificeerd middels een uitvoeringsverordening. De informatie die voor notificatie nodig is, wordt in de onderhavige regeling nader uitgewerkt. Het indienen van de benodigde informatie bij Enisa vergt van de NCCA (RDI) een tijdsbesteding van circa 1 uur. Voor organisaties die de informatie aan de NCCA moeten aanleveren, wordt verwacht dat zij circa 1 uur besteden aan de interne administratieve verwerking en afhandeling van de door de RDI verrichte notificatie.

Verwachting

Op basis van de inschatting dat er drie certificeringsinstanties en zeven ITSEF's zijn, wordt verwacht dat er in het komende jaar tien initiële aanvragen zullen worden ingediend. Thans bestaat geen concreet zicht op het aantal nieuwe aanvragen. Voor de daaropvolgende jaren kan niet worden uitgesloten dat alsnog aanvragen worden ingediend. Zoals aangegeven dient er jaarlijks een beoordeling te worden uitgevoerd ten behoeve van zowel de accreditatie als de autorisatie.

Tegen het besluit tot (afwijzing van) autorisatie door een NCCA staan bezwaar en beroep open. Op basis van ervaringscijfers van een vergelijkbaar nationaal schema worden geen bezwaar- of beroepsprocedures verwacht en zijn de regeldrukeffecten dus verwaarloosbaar.

Initiële kosten

De tijdsbesteding per organisatie wordt ingeschat op 17–73 uur. Dat betreft 16 uur voor de autorisatie en 1 uur voor de interne administratieve verwerking en afhandeling van de door de RDI verrichte notificatie. Uitgaande van een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op een kostenraming van € 918,– tot € 3.942,–.

Indien ter plaatse onderzoek op locatie dient te worden uitgevoerd, worden per locatie bijkomende kosten van € 864,– tot € 1.728,– (16 tot 32 uur) in rekening gebracht.

Als rekening wordt gehouden met tien initiële aanvragen lopen de totale initiële kosten op tot tussen de € 9.180,– en € 39.420,–. Hierbij is rekening gehouden met één locatie.

Jaarlijkse kosten

De jaarlijkse tijdsbesteding per organisatie zonder significate wijzigingen wordt ingeschat op 1 uur. Uitgaande van een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 54,–.

De jaarlijkse tijdsbesteding per organisatie met één locatie en significante wijzigingen wordt tussen de 17 en 32 uur ingeschat. Uitgaande van een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 918,– tot € 1.728,–.

Als rekening wordt gehouden met tien organisaties waarbij geen significante wijzigingen zijn lopen de totale jaarlijkse kosten lopen op tot € 540,–.

Als er wel significante wijzigingen plaatsvinden kunnen de jaarlijkse totale kosten oplopen tot € 17.280,–. Hierbij is rekening gehouden met één locatie.

4. Uitvoerbaarheid en handhaafbaarheid

De RDI heeft een Uitvoerings- en handhaafbaarheidstoets uitgevoerd en acht de regeling en bijbehorende toezichtstaken uitvoerbaar, handhaafbaar en fraudebestendig.

5. Notificatie

Onderhavige regeling bevat geen technische voorschriften in de zin van richtlijn (EU) nr. 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij.

[3] https://www.rva.nl/nieuws/samenwerking-rijksinspectie-digitale-infrastructuur-rdi-en-raad-voor-accreditatie-rva/

6. Consultatie

De doelgroep van de regeling is nauw betrokken geweest bij de totstandkoming van de EUCC en is daarnaast informeel geraadpleegd bij het opstellen van deze regeling. Een internetconsultatie is daarom niet gehouden. Bovendien strekt de regeling tot uitvoering van een EU-verordening, waardoor zij valt onder een van de uitzonderingen op het kabinetsbeleid inzake internetconsultatie.

Naar aanleiding van de gevoerde raadpleging met verschillende certificeringsinstanties en ITSEF's is overeengekomen om in de toekomst regelmatig in gesprek te blijven met de betrokken stakeholders. Dit overleg zal bijdragen aan een continue afstemming en het bevorderen van wederzijds begrip, zodat gezamenlijke doelstellingen effectief kunnen worden nagestreefd.

7. Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst. Hiermee wordt afgeweken van de vaste verandermomenten, zoals opgenomen in het kabinetsbeleid inzake vaste verandermomenten (Kamerstukken II 2009/10, 29 515, nr. 309). Het kabinetsbeleid biedt de mogelijkheid af te wijken van vaste verandermomenten indien nodig voor de implementatie van Europese regelgeving.

De Minister van Economische Zaken,
V.P.G. Karremans