BESLUIT (EU, Euratom) 2021/259 VAN DE COMMISSIE

van 10 februari 2021

tot vaststelling van uitvoeringsbepalingen inzake industriële beveiliging met betrekking tot gerubriceerde subsidies

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 249,

Gezien het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie, en met name artikel 106,

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

Gezien Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie ([2]),

Gezien Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie ([3]),

Gezien Besluit (EU, Euratom) 2017/46 van de Commissie van 10 januari 2017 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie ([4]),

Na raadpleging van de deskundigengroep voor veiligheid van de Commissie, overeenkomstig artikel 41, lid 5, van Besluit (EU, Euratom) 2015/444,

Overwegende hetgeen volgt:

(1) In de artikelen 41, 42, 47 en 48 van Besluit (EU, Euratom) 2015/444 wordt bepaald dat er meer gedetailleerde bepalingen ter aanvulling en ondersteuning van hoofdstuk 6 van dat besluit moeten worden vastgesteld in uitvoeringsbepalingen inzake industriële beveiliging, die betrekking hebben op kwesties zoals de toekenning van gerubriceerde subsidieovereenkomsten, veiligheidsverklaringen voor een vestiging, veiligheidsverklaringen voor personeel, bezoeken, overdracht en vervoer van gerubriceerde informatie van de Europese Unie ("EUCI").

(2) In Besluit (EU, Euratom) 2015/444 wordt bepaald dat gerubriceerde subsidieovereenkomsten moeten worden uitgevoerd in nauwe samenwerking met de nationale veiligheidsautoriteiten, de aangewezen veiligheidsautoriteiten of andere bevoegde autoriteiten van de betrokken lidstaten. De lidstaten zijn overeengekomen ervoor te zorgen dat elke onder hun bevoegdheid vallende entiteit die gerubriceerde informatie afkomstig van de Commissie kan ontvangen of genereren, een gedegen veiligheidsonderzoek heeft ondergaan en een passende bescherming kan bieden die gelijkwaardig is aan de bescherming die door de veiligheidsvoorschriften van de Raad van de Europese Unie wordt geboden voor de bescherming van gerubriceerde EU-informatie welke een overeenkomstige rubricering draagt, zoals bepaald in de Overeenkomst tussen de lidstaten van de Europese Unie, in het kader van de Raad bijeen, betreffende de bescherming van in het belang van de Europese Unie uitgewisselde gerubriceerde informatie (2011/C 202/05) ([5]).

([1]) PB L 193 van 30.7.2018, blz. 1.
([2]) PB L 72 van 17.3.2015, blz. 41.
([3]) PB L 72 van 17.3.2015, blz. 53.
([4]) PB L 6 van 11.1.2017, blz. 40.
([5]) PB C 202 van 8.7.2011, blz. 13.

(3) De Raad, de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid zijn overeengekomen te zorgen voor maximale consistentie bij de toepassing van beveiligingsvoorschriften betreffende de bescherming van EUCI, rekening houdend met hun specifieke institutionele en organisatorische behoeften, conform de verklaringen die zijn gehecht aan de notulen van de Raadszitting waarop Besluit 2013/488/EU van de Raad ([6]) betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie is aangenomen.

(4) De uitvoeringsbepalingen van de Commissie inzake industriële beveiliging met betrekking tot gerubriceerde subsidies moeten bijgevolg ook een maximale consistentie waarborgen en rekening houden met de op 13 december 2016 door het beveiligingscomité van de Raad goedgekeurde richtsnoeren inzake industriële beveiliging.

(5) Op 4 mei 2016 heeft de Commissie een besluit ([7]) vastgesteld waarbij het voor veiligheid bevoegde Commissielid wordt gemachtigd om namens de Commissie en onder haar verantwoordelijkheid de in artikel 60 van Besluit (EU, Euratom) 2015/444 bedoelde uitvoeringsbepalingen vast te stellen,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

HOOFDSTUK 1

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. In dit besluit worden uitvoeringsbepalingen inzake industriële beveiliging met betrekking tot gerubriceerde subsidies vastgesteld zoals bedoeld in Besluit (EU, Euratom) 2015/444 en met name hoofdstuk 6 van dat besluit.

2. In dit besluit worden specifieke vereisten vastgesteld voor de bescherming van gerubriceerde EU-informatie (EUCI) in de bekendmakingen van oproepen en bij de toekenning van subsidies en de uitvoering van gerubriceerde subsidieovereenkomsten die door de Europese Commissie worden gesloten.

3. Dit besluit is van toepassing op subsidies waarmee informatie met de volgende rubriceringsniveaus gemoeid is:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

4. Dit besluit is van toepassing onverminderd de specifieke regels die zijn vastgesteld in andere rechtshandelingen, zoals die betreffende het industrieel ontwikkelingsprogramma voor de Europese defensie.

Artikel 2

Verantwoordelijkheden binnen de Commissie

1. In het kader van de in Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad beschreven verantwoordelijkheden van de ordonnateur van de subsidieverlenende autoriteit, zorgt de betrokken ordonnateur ervoor dat de gerubriceerde subsidie voldoet aan Besluit (EU, Euratom) 2015/444 en de uitvoeringsbepalingen daarvan.

([6]) Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 274 van 15.10.2013, blz. 1).

([7]) Besluit van de Commissie van 4 mei 2016 betreffende een machtiging inzake veiligheid (C(2016) 2797 final).

2. Daartoe wint de betrokken ordonnateur in alle stadia het advies in van de veiligheidsautoriteit van de Commissie over kwesties in verband met de beveiligingselementen van een gerubriceerde subsidieovereenkomst, een gerubriceerd programma of een gerubriceerd project en stelt hij de lokale veiligheidsagent in kennis van de ondertekende gerubriceerde subsidieovereenkomsten. De beslissing over het rubriceringsniveau van specifieke onderwerpen berust bij de subsidieverlenende autoriteit en wordt genomen met inachtneming van de rubriceringsgids.

3. Wanneer de in artikel 5, lid 3, bedoelde programma- of projectbeveiligingsinstructies worden toegepast, kwijten de subsidieverlenende autoriteit en de veiligheidsautoriteit van de Commissie zich van de verantwoordelijkheden die hun in die instructies zijn toegewezen.

4. Bij de inachtneming van de vereisten van deze uitvoeringsbepalingen werkt de veiligheidsautoriteit van de Commissie nauw samen met de nationale veiligheidsautoriteiten en de aangewezen veiligheidsautoriteiten van de betrokken lidstaten, met name wat betreft de veiligheidsverklaringen voor een vestiging, de veiligheidsverklaringen voor personeel, de procedures voor bezoeken en de vervoerplannen.

5. Wanneer subsidies worden beheerd door uitvoerende agentschappen of andere financieringsorganen van de EU en de specifieke regels van andere in artikel 1, lid 4, bedoelde rechtshandelingen niet van toepassing zijn:

a) oefent de delegerende afdeling van de Commissie de rechten uit die gerelateerd zijn aan de bron van EUCI die in het kader van de subsidies wordt gegenereerd, indien de delegatieregelingen daarin voorzien;

b) is de delegerende afdeling van de Commissie verantwoordelijk voor het bepalen van de rubriceringsgraad;

c) worden verzoeken om informatie over veiligheidsverklaringen en kennisgevingen aan nationale veiligheidsautoriteiten en/of aangewezen veiligheidsautoriteiten verzonden via de veiligheidsautoriteit van de Commissie.

HOOFDSTUK 2

BEHANDELING VAN OPROEPEN VOOR GERUBRICEERDE SUBSIDIES

Artikel 3

Basisbeginselen

1. Gerubriceerde delen van de subsidies worden alleen uitgevoerd door in een lidstaat geregistreerde begunstigden, of door in een derde land geregistreerde of door door een internationale organisatie opgerichte begunstigden wanneer dat derde land of die internationale organisatie een informatiebeveiligingsovereenkomst met de Europese Unie heeft gesloten of een administratieve regeling heeft getroffen met de Commissie ([8]).

2. Voorafgaand aan de oproep voor een gerubriceerde subsidie bepaalt de subsidieverlenende autoriteit het rubriceringsniveau van alle informatie die aan aanvragers kan worden verstrekt. De subsidieverlenende autoriteit bepaalt ook het maximale rubriceringsniveau van alle informatie die bij de uitvoering van de subsidieovereenkomst, het programma of het project wordt gebruikt of gegenereerd, of ten minste de verwachte omvang en het verwachte type van de op te stellen of te behandelen informatie, en de noodzaak van een gerubriceerd communicatie- en informatiesysteem.

3. De subsidieverlenende autoriteit zorgt ervoor dat er in de oproepen voor gerubriceerde subsidies informatie wordt verstrekt over de bijzondere beveiligingsverplichtingen in verband met gerubriceerde informatie. In de documentatie bij de oproep wordt toegelicht binnen welke termijn de begunstigden de veiligheidsverklaringen voor een vestiging moeten verkrijgen, voor zover dit vereist is. De bijlagen I en II bevatten voorbeelden van templates voor informatie over de voorwaarden van de oproep.

([8]) De lijst van de door de Europese Unie gesloten overeenkomsten en de door de Europese Commissie getroffen administratieve regelingen, op grond waarvan gerubriceerde EU-informatie kan worden uitgewisseld met derde landen en internationale organisaties, is te vinden op de website van de Commissie.

4. De subsidieverlenende autoriteit zorgt ervoor dat informatie met rubricering RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET pas aan de aanvragers wordt bekendgemaakt nadat zij een niet-openbaarmakingsovereenkomst hebben ondertekend, waarin aanvragers ertoe worden verplicht EUCI te behandelen en te beschermen conform Besluit (EU, Euratom) 2015/444, de uitvoeringsbepalingen daarvan en de toepasselijke nationale voorschriften.

5. Wanneer er informatie met rubricering RESTREINT UE/EU RESTRICTED aan aanvragers wordt verstrekt, worden de in artikel 5, lid 7, van dat besluit vermelde minimumvereisten opgenomen in de oproep of in de niet-openbaarmakingsregelingen die in de fase van het voorstel worden gesloten.

6. Alle aanvragers en begunstigden die verplicht zijn om informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET in hun vestigingen te behandelen of op te slaan, hetzij in de fase van het voorstel, hetzij tijdens de uitvoering van de gerubriceerde subsidieovereenkomst zelf, zijn in het bezit van een veiligheidsverklaring voor een vestiging van het vereiste niveau, behalve in de in lid 9 genoemde gevallen. Hieronder worden de drie scenario's geschetst die zich kunnen voordoen in de fase van het voorstel voor een gerubriceerde subsidie waarbij EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gemoeid is:

a) geen toegang tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET in de fase van het voorstel:

   wanneer de oproep een subsidie betreft waarbij EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gemoeid is, maar waarbij de aanvrager niet verplicht is deze informatie in de fase van het voorstel te behandelen, wordt een aanvrager die niet in het bezit is van een veiligheidsverklaring voor een vestiging van het vereiste niveau, niet van de aanvraagprocedure uitgesloten op grond van het feit dat hij niet in het bezit is van een dergelijke veiligheidsverklaring;

b) toegang tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET in de bedrijfsruimten van de subsidieverlenende autoriteit in de fase van het voorstel:

   toegang wordt verleend aan het personeel van de aanvrager dat in het bezit is van een veiligheidsverklaring voor personeel van het vereiste niveau en dat een "noodzaak tot kennisname" heeft;

c) behandeling of opslag van EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET in de bedrijfsruimten van de aanvrager in de fase van het voorstel:

   wanneer aanvragers ingevolge de oproep in hun bedrijfsruimten EUCI moeten behandelen of opslaan, is de aanvrager in het bezit van een veiligheidsverklaring voor een vestiging van het vereiste niveau. In dergelijke omstandigheden krijgt de subsidieverlenende autoriteit, via de veiligheidsautoriteit van de Commissie, van de desbetreffende nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit de garantie dat er aan de aanvrager een passende veiligheidsverklaring voor een vestiging is verleend en zulks vóór de verstrekking van EUCI-materiaal aan de aanvrager. Toegang wordt verleend aan het personeel van de aanvrager dat in het bezit is van een veiligheidsverklaring voor personeel van het vereiste niveau en dat een "noodzaak tot kennisname" heeft.

7. Een veiligheidsverklaring voor een vestiging of een veiligheidsverklaring voor personeel is in beginsel niet vereist voor toegang tot informatie met rubricering RESTREINT UE/EU RESTRICTED, noch in de fase van het voorstel, noch voor de uitvoering van subsidieovereenkomst. Wanneer de lidstaten op grond van hun nationale wet- en regelgeving een veiligheidsverklaring voor een vestiging of een veiligheidsverklaring voor personeel verlangen voor subsidieovereenkomsten of subcontracten op het niveau RESTREINT UE/EU RESTRICTED (zie bijlage IV), leggen die nationale voorschriften geen aanvullende verplichtingen op aan andere lidstaten, of sluiten die voorschriften aanvragers, begunstigden of subcontractanten van lidstaten waar er geen dergelijke voorschriften inzake een veiligheidsverklaring voor een vestiging of een veiligheidsverklaring voor personeel bestaan voor toegang tot informatie met rubricering RESTREINT UE/EU RESTRICTED, niet uit van de desbetreffende subsidieovereenkomsten/subcontracten of van mededinging op dat gebied. Deze subsidieovereenkomsten worden in de lidstaten uitgevoerd overeenkomstig hun nationale wet- en regelgeving.

8. Indien er een veiligheidsverklaring voor een vestiging is vereist voor de behandeling van een oproep en voor de uitvoering van een gerubriceerde subsidieovereenkomst, dient de subsidieverlenende autoriteit, via de veiligheidsautoriteit van de Commissie, een verzoek in bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de begunstigde, waarbij gebruik wordt gemaakt van een informatieblad voor de veiligheidsverklaring voor een vestiging of een ander soortgelijk elektronisch formulier. Bijlage III, aanhangsel D, bevat een voorbeeld van een informatieblad voor de veiligheidsverklaring voor een vestiging ([9]). De reactie op een informatieblad voor de veiligheidsverklaring voor een vestiging wordt, voor zover mogelijk, binnen tien werkdagen na de datum van het verzoek verstrekt.

9. Wanneer overheidsinstellingen van de lidstaten of instellingen onder toezicht van de overheid deelnemen aan gerubriceerde subsidies waarvoor veiligheidsverklaringen voor een vestiging vereist zijn, en wanneer er voor deze instellingen geen veiligheidsverklaringen voor een vestiging zijn afgegeven op grond van de nationale wetgeving, gaat de subsidieverlenende autoriteit, via de veiligheidsautoriteit van de Commissie, bij de betrokken nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit na of deze instellingen in staat zijn om EUCI op het vereiste niveau te behandelen.

([9]) Andere formulieren kunnen qua ontwerp afwijken van het voorbeeld in deze uitvoeringsbepalingen.

10. Indien er een veiligheidsverklaring voor personeel is vereist voor de uitvoering van een gerubriceerde subsidieovereenkomst en wanneer er volgens de nationale voorschriften een veiligheidsverklaring voor een vestiging noodzakelijk is voordat er een veiligheidsverklaring voor personeel wordt toegekend, gaat de subsidieverlenende autoriteit, via de veiligheidsautoriteit van de Commissie en met behulp van een informatieblad voor de veiligheidsverklaring voor een vestiging, bij de betrokken nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de begunstigde na of de begunstigde in het bezit is van een veiligheidsverklaring voor een vestiging dan wel of de procedure voor de toekenning daarvan aan de gang is. In dat geval geeft de Commissie geen verzoeken om veiligheidsverklaringen voor personeel af met behulp van het informatieblad voor de veiligheidsverklaring voor personeel.

Artikel 4

Uitbesteding bij gerubriceerde subsidies

1. De voorwaarden waaronder begunstigden actietaken waarbij EUCI gemoeid is, mogen uitbesteden worden in de oproep en in de subsidieovereenkomst vastgesteld. Deze voorwaarden omvatten het vereiste dat alle informatiebladen voor de veiligheidsverklaring voor een vestiging via de veiligheidsautoriteit van de Commissie worden ingediend. Voor uitbesteding is de voorafgaande schriftelijke toestemming van de subsidieverlenende autoriteit vereist. In voorkomend geval is de uitbesteding in overeenstemming met het basisbesluit tot vaststelling van het programma.

2. Gerubriceerde delen van de subsidies worden alleen uitbesteed aan in een lidstaat geregistreerde entiteiten, of door in een derde land geregistreerde of door door een internationale organisatie opgerichte entiteiten wanneer dat derde land of die internationale organisatie een informatiebeveiligingsovereenkomst met de Europese Unie heeft gesloten of een administratieve regeling heeft getroffen met de Commissie ([10]).

HOOFDSTUK 3

BEHANDELING VAN GERUBRICEERDE SUBSIDIES

Artikel 5

Basisbeginselen

1. Bij de toekenning van een gerubriceerde subsidie zorgt de subsidieverlenende autoriteit er samen met de veiligheidsautoriteit van de Commissie voor dat de verplichtingen van de begunstigden met betrekking tot de bescherming van EUCI die bij de uitvoering van de subsidieovereenkomst wordt gebruikt of gegenereerd, een integrerend onderdeel vormen van de subsidieovereenkomst. De specifieke veiligheidsvereisten voor de subsidie hebben de vorm van een memorandum over de beveiligingsaspecten. Bijlage III bevat een voorbeeld van een template voor een memorandum over de beveiligingsaspecten.

2. Alvorens een gerubriceerde subsidie te ondertekenen, keurt de subsidieverlenende autoriteit een rubriceringsgids goed voor de taken die moeten worden uitgevoerd en de informatie die wordt gegenereerd bij de uitvoering van de subsidie, of, in voorkomend geval, op programma- of projectniveau. De rubriceringsgids is een onderdeel van het memorandum over de beveiligingsaspecten.

3. De specifieke veiligheidsvereisten voor het programma of het project hebben de vorm van beveiligingsinstructies voor een programma (of project). De beveiligingsinstructies voor een programma (of project) kunnen worden opgesteld aan de hand van de bepalingen van de in bijlage III opgenomen template voor het memorandum over de beveiligingsaspecten. Die beveiligingsinstructies worden ontwikkeld door de afdeling van de Commissie die het programma of het project beheert, in nauwe samenwerking met de veiligheidsautoriteit van de Commissie, en worden voor advies voorgelegd aan de deskundigengroep voor veiligheid van de Commissie. Wanneer een subsidieovereenkomst deel uitmaakt van een programma of een project met eigen beveiligingsinstructies voor een programma (of project), heeft het memorandum over de beveiligingsaspecten een vereenvoudigde vorm en bevat het een verwijzing naar de beveiligingsbepalingen van de beveiligingsinstructies van het programma of het project.

4. Behalve in de in artikel 3, lid 9, genoemde gevallen, wordt de gerubriceerde subsidieovereenkomst pas ondertekend nadat de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de aanvrager de veiligheidsverklaring voor een vestiging van de aanvrager heeft bevestigd of, indien de gerubriceerde subsidieovereenkomst aan een consortium wordt toegekend, totdat de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van ten minste één aanvrager, binnen het consortium, of indien nodig van meerdere aanvragers, de veiligheidsverklaring voor een vestiging van de aanvrager heeft bevestigd.

5. In beginsel, en tenzij anders bepaald in andere relevante voorschriften, wordt de subsidieverlenende autoriteit beschouwd als de bron van EUCI die bij de uitvoering van de subsidieovereenkomst wordt gegenereerd.

([10]) De lijst van de door de Europese Unie gesloten overeenkomsten en de door de Europese Commissie getroffen administratieve regelingen, op grond waarvan gerubriceerde EU-informatie kan worden uitgewisseld met derde landen en internationale organisaties, is te vinden op de website van de Commissie.

6. De subsidieverlenende autoriteit stelt, via de veiligheidsautoriteit van de Commissie, de nationale veiligheidsautoriteiten en/of de aangewezen veiligheidsautoriteiten van alle begunstigden en subcontractanten in kennis van de ondertekening van gerubriceerde subsidieovereenkomsten of subcontracten en van de verlenging of vroegtijdige beëindiging van dergelijke subsidieovereenkomsten of subcontracten. Een lijst van de vereisten per land is opgenomen in bijlage IV.

7. Subsidieovereenkomsten waarbij informatie met rubricering RESTREINT UE/EU RESTRICTED gemoeid is, bevatten een beveiligingsclausule die de bepalingen van bijlage III, aanhangsel E, bindend maakt voor de begunstigden. Deze subsidieovereenkomsten bevatten een memorandum over de beveiligingsaspecten, waarin minimaal de vereisten voor de behandeling van informatie met rubricering RESTREINT UE/EU RESTRICTED zijn opgenomen, met inbegrip van informatieborgingaspecten en specifieke vereisten waaraan door de begunstigden moet worden voldaan met betrekking tot de homologatie van hun communicatie- en informatiesystemen waarin informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld.

8. Wanneer de nationale wet- en regelgeving van de lidstaten dit vereist, zorgen de nationale veiligheidsautoriteiten of de aangewezen veiligheidsautoriteiten ervoor dat onder hun bevoegdheid vallende begunstigden of subcontractanten de toepasselijke beveiligingsbepalingen voor de bescherming van informatie met rubricering RESTREINT UE/EU RESTRICTED in acht nemen en brengen zij controlebezoeken aan vestigingen van begunstigden of subcontractanten op hun grondgebied. Indien de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit niet aan een dergelijke verplichting is onderworpen, zorgt de subsidieverlenende autoriteit ervoor dat de begunstigden de voorgeschreven beveiligingsbepalingen van bijlage III, aanhangsel E, toepassen.

Artikel 6

Toegang tot EUCI voor personeel van begunstigden en subcontractanten

1. De subsidieverlenende autoriteit zorgt ervoor dat gerubriceerde subsidieovereenkomsten bepalingen bevatten die stipuleren dat het personeel van begunstigden of subcontractanten dat voor de uitvoering van de gerubriceerde subsidieovereenkomst of het gerubriceerde subcontract toegang nodig heeft tot EUCI, deze toegang alleen krijgt indien:

a) voor de betrokkene de noodzaak tot kennisname is vastgesteld;

b) voor informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET door de respectieve nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit of een andere bevoegde veiligheidsautoriteit aan de betrokkene een veiligheidsverklaring van het vereiste niveau is afgegeven;

c) de betrokkene is geïnstrueerd over de toepasselijke beveiligingsvoorschriften voor de bescherming van EUCI en hij zijn verantwoordelijkheden in verband met de bescherming van dergelijke informatie heeft bevestigd.

2. In voorkomend geval is de toegang tot EUCI ook in overeenstemming met het basisbesluit tot vaststelling van het programma en wordt er ook rekening gehouden met eventuele aanvullende markeringen die in de rubriceringsgids zijn gedefinieerd.

3. Indien een begunstigde of subcontractant een onderdaan van een niet-EU-land in dienst wil nemen voor een functie waarvoor toegang tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET is vereist, is het de verantwoordelijkheid van de begunstigde of subcontractant om de procedure voor het verkrijgen van een veiligheidsverklaring voor een dergelijke persoon in te leiden overeenkomstig de nationale wet- en regelgeving die van toepassing is op de plaats waar de toegang tot de EUCI zal worden verleend.

Artikel 7

Toegang tot EUCI door deskundigen die deelnemen aan controles, evaluaties of audits

1. Wanneer externe personen ("deskundigen") betrokken zijn bij controles, evaluaties of audits door de subsidieverlenende autoriteit of bij prestatie-evaluaties van de begunstigden welke toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET vereisen, krijgen zij alleen een overeenkomst indien door de respectieve nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit of een andere bevoegde veiligheidsautoriteit aan hen een veiligheidsverklaring van het vereiste niveau is afgegeven. De subsidieverlenende autoriteit voert, via de veiligheidsautoriteit van de Commissie, de verificaties uit en verzoekt de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit om, indien nodig, het doorlichtingsproces voor deskundigen op gang te brengen; zulks ten minste zes maanden vóór de aanvang van hun respectieve overeenkomsten.

2. Vóór de ondertekening van hun overeenkomsten, worden de deskundigen geïnstrueerd over de toepasselijke beveiligingsvoorschriften voor de bescherming van EUCI en hebben zij hun verantwoordelijkheden in verband met de bescherming van dergelijke informatie erkend.

HOOFDSTUK 4

BEZOEKEN IN VERBAND MET GERUBRICEERDE SUBSIDIEOVEREENKOMSTEN

Artikel 8

Basisbeginselen

1. Wanneer de subsidieverlenende autoriteit, de deskundigen, de begunstigden of de subcontractanten in het kader van de uitvoering van een gerubriceerde subsidieovereenkomst in elkaars bedrijfsruimten toegang moeten hebben tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, worden er, in overleg met de nationale veiligheidsautoriteiten of de aangewezen veiligheidsautoriteiten of andere bevoegde veiligheidsautoriteiten, bezoeken georganiseerd.

2. Voor de in lid 1 bedoelde bezoeken gelden de volgende vereisten:

a) het bezoek heeft een officieel doel in verband met de gerubriceerde subsidie;

b) elke bezoeker is in het bezit van een veiligheidsverklaring voor personeel van het vereiste niveau en de noodzaak tot kennisname staat vast, teneinde toegang te krijgen tot EUCI die wordt gebruikt of gegenereerd bij de uitvoering van de gerubriceerde subsidie.

Artikel 9

Aanvragen voor bezoeken

1. Bezoeken van begunstigden of subcontractanten aan vestigingen van andere begunstigden of subcontractanten of aan bedrijfsruimten van de subsidieverlenende autoriteit die toegang behelzen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, worden conform de volgende procedure geregeld:

a) de veiligheidsagent van de vestiging die de bezoeker stuurt, vult alle relevante onderdelen van het aanvraagformulier voor een bezoek in en dient de aanvraag in bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de vestiging. Een template van het aanvraagformulier voor een bezoek is opgenomen in bijlage III, aanhangsel C;

b) de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de verzendende vestiging moet de veiligheidsverklaring voor personeel van de bezoeker bevestigen voordat de aanvraag voor een bezoek wordt ingediend bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging (of de veiligheidsautoriteit van de Commissie in het geval van een bezoek aan de bedrijfsruimten van een subsidieverlenende autoriteit);

c) de veiligheidsagent van de verzendende vestiging ontvangt vervolgens, via zijn nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit, het antwoord van de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging (of de veiligheidsautoriteit van de Commissie), die de aanvraag voor een bezoek goedkeurt of afwijst;

d) een aanvraag voor een bezoek wordt geacht te zijn goedgekeurd als er tot vijf werkdagen vóór de datum van het bezoek geen bezwaar wordt gemaakt.

2. Bezoeken van ambtenaren van de subsidieverlenende autoriteit, deskundigen of auditors aan vestigingen van de begunstigden of subcontractanten die toegang behelzen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, worden conform de volgende procedure geregeld:

a) de bezoeker vult alle relevante onderdelen van het aanvraagformulier voor een bezoek in en dient het in bij de veiligheidsautoriteit van de Commissie;

b) de veiligheidsautoriteit van de Commissie bevestigt de veiligheidsverklaring voor personeel van de bezoeker voordat de aanvraag voor een bezoek wordt ingediend bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging;

c) de veiligheidsautoriteit van de Commissie ontvangt een antwoord van de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging, die de aanvraag voor een bezoek goedkeurt of afwijst;

d) een aanvraag voor een bezoek wordt geacht te zijn goedgekeurd als er tot vijf werkdagen vóór de datum van het bezoek geen bezwaar wordt gemaakt.

3. Een aanvraag voor een bezoek kan betrekking hebben op een enkel bezoek of op herhaalde bezoeken. In het geval van herhaalde bezoeken kan de aanvraag voor een bezoek tot één jaar geldig zijn vanaf de gevraagde startdatum.

4. De geldigheidsduur van een aanvraag voor een bezoek overschrijdt niet de geldigheidsduur van de veiligheidsverklaring voor personeel van de bezoeker.

5. Als algemene regel geldt dat een aanvraag voor een bezoek ten minste 15 werkdagen vóór de datum van het bezoek wordt ingediend bij de bevoegde veiligheidsautoriteit van de ontvangende vestiging.

Artikel 10

Procedures voor bezoeken

1. Alvorens de bezoekers toegang te verlenen tot EUCI, zorgt de veiligheidsdienst van de ontvangende vestiging voor de inachtneming van alle met het bezoek verband houdende beveiligingsprocedures en -regels die door zijn nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit zijn vastgesteld.

2. Bezoekers bewijzen bij aankomst in de ontvangende vestiging hun identiteit door een geldige identiteitskaart of een geldig paspoort over te leggen. De identificatiegegevens stemmen overeen met de in de aanvraag voor een bezoek verstrekte gegevens.

3. De ontvangende vestiging zorgt ervoor dat er een register wordt bijgehouden van alle bezoekers, met daarin hun naam, de organisatie die zij vertegenwoordigen, de datum waarop de veiligheidsverklaring voor personeel verstrijkt, de datum van het bezoek en de namen van de bezochte personen. Dit register wordt gedurende een periode van ten minste vijf jaar bewaard, of langer indien de nationale regelgeving van het land van de ontvangende vestiging dit vereist.

Artikel 11

Rechtstreeks geregelde bezoeken

1. In het kader van specifieke projecten kunnen de desbetreffende nationale veiligheidsautoriteiten of aangewezen veiligheidsautoriteiten en de veiligheidsautoriteit van de Commissie in onderling overleg een procedure vaststellen op grond waarvan bezoeken in verband met een specifieke gerubriceerde subsidie rechtstreeks kunnen worden geregeld tussen de veiligheidsagent van de bezoeker en de veiligheidsagent van de te bezoeken vestiging. Een template van het daarvoor te gebruiken formulier is opgenomen in bijlage III, aanhangsel C. Een dergelijke uitzonderlijke procedure wordt beschreven in de beveiligingsinstructies voor een programma (of project) of in andere specifieke regelingen. In dergelijke gevallen zijn de procedures van artikel 9 en artikel 10, lid 1, niet van toepassing.

2. Bezoeken die toegang behelzen tot informatie met rubricering RESTREINT UE/EU RESTRICTED, worden rechtstreeks tussen de verzendende en de ontvangende entiteit geregeld, zonder dat de procedures van artikel 9 en artikel 10, lid 1, hoeven te worden gevolgd.

HOOFDSTUK 5

OVERDRACHT EN VERVOER VAN EUCI BIJ DE UITVOERING VAN GERUBRICEERDE SUBSIDIEOVEREENKOMSTEN

Artikel 12

Basisbeginselen

De subsidieverlenende autoriteit zorgt ervoor dat alle besluiten in verband met de overdracht en het vervoer van EUCI in overeenstemming zijn met Besluit (EU, Euratom) 2015/444 en de uitvoeringsbepalingen daarvan, en met de voorwaarden van de gerubriceerde subsidieovereenkomst, met inbegrip van de toestemming van de bron ervan.

Artikel 13

Elektronische behandeling

1. De elektronische behandeling en overdracht van EUCI wordt uitgevoerd in overeenstemming met de hoofdstukken 5 en 6 van Besluit (EU, Euratom) 2015/444 en de uitvoeringsbepalingen daarvan.

De communicatie- en informatiesystemen die eigendom zijn van een begunstigde en die worden gebruikt voor de behandeling van EUCI in het kader van de uitvoering van de subsidieovereenkomst, worden gehomologeerd door de bevoegde veiligheidshomologatieautoriteit. Elke elektronische overdracht van EUCI wordt beschermd door encryptieproducten die zijn goedgekeurd overeenkomstig artikel 36, lid 4, van Besluit (EU, Euratom) 2015/444. TEMPEST-beveiligingsmaatregelen worden uitgevoerd overeenkomstig artikel 36, lid 6, van dat besluit.

2. De veiligheidshomologatie van het communicatie- en informatiesysteem van de begunstigde waarin EUCI met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld en van de eventuele koppeling daarvan, kan worden gedelegeerd aan de veiligheidsagent van een begunstigde indien de nationale wet- en regelgeving dit toestaat. Wanneer die taak wordt gedelegeerd, is de begunstigde verantwoordelijk voor de uitvoering van de minimale veiligheidsvoorschriften die in het memorandum over de beveiligingsaspecten zijn beschreven voor de behandeling van informatie met rubricering RESTREINT UE/EU RESTRICTED in zijn communicatie- en informatiesysteem. De desbetreffende nationale veiligheidsautoriteiten of aangewezen veiligheidsautoriteiten en veiligheidshomologatieautoriteiten blijven echter verantwoordelijk voor de bescherming van de door de begunstigde behandelde informatie met rubricering RESTREINT UE/EU RESTRICTED en behouden het recht om de door de begunstigde genomen beveiligingsmaatregelen te controleren. Bovendien verstrekt de begunstigde de subsidieverlenende autoriteit en, indien dit is vereist krachtens de nationale wet- en regelgeving, de bevoegde nationale veiligheidshomologatieautoriteit een verklaring van overeenstemming, waarin wordt gecertificeerd dat het communicatie- en informatiesysteem van de begunstigde en de bijbehorende koppelingen zijn gehomologeerd voor de behandeling van EUCI met rubricering RESTREINT UE/EU RESTRICTED ([11]).

Artikel 14

Vervoer door commerciële koeriers

Bij het vervoer van EUCI door commerciële koeriers worden de relevante bepalingen van Besluit (EU, Euratom) 2019/1962 van de Commissie ([12]) houdende uitvoeringsbepalingen voor de omgang met RESTREINT UE/EU RESTRICTED-informatie en Besluit (EU, Euratom) 2019/1961 van de Commissie ([13]) houdende uitvoeringsbepalingen voor de omgang met CONFIDENTIEL UE/EU CONFIDENTIAL- en SECRET UE/EU SECRET-informatie in acht genomen.

Artikel 15

Vervoer in handbagage

1. Voor het vervoer van gerubriceerde informatie in handbagage gelden er strenge veiligheidsvereisten.

2. Personeel van de begunstigde mag informatie met rubricering RESTREINT UE/EU RESTRICTED binnen de Unie vervoeren in handbagage, mits aan de volgende vereisten wordt voldaan:

a) de gebruikte envelop/verpakking is ondoorzichtig en daarop is geen vermelding aangebracht betreffende de rubricering van de inhoud ervan;

b) de drager geeft de gerubriceerde informatie niet uit handen;

c) de envelop of verpakking wordt onderweg niet geopend.

3. Voor informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET wordt het vervoer in handbagage door personeel van de begunstigde binnen een lidstaat vooraf geregeld tussen de verzendende en de ontvangende entiteiten. De verzendende autoriteit of vestiging stelt de ontvangende autoriteit of vestiging in kennis van de gegevens van de zending, met inbegrip van de referentie, de rubricering, het verwachte tijdstip van aankomst en de naam van de koerier. Dit vervoer in handbagage is toegestaan, mits aan de volgende vereisten wordt voldaan:

a) de gerubriceerde informatie wordt vervoerd in een dubbele envelop/verpakking;

b) de buitenste envelop/verpakking is beveiligd en daarop is geen vermelding aangebracht van de rubricering van de inhoud ervan, terwijl op de binnenste envelop het rubriceringsniveau is vermeld;

c) de drager geeft de EUCI niet uit handen;

d) de envelop of verpakking wordt onderweg niet geopend;

e) de envelop/verpakking wordt vervoerd in een afsluitbare aktetas of een soortgelijk goedgekeurd opbergmiddel van een zodanige omvang en gewicht dat het te allen tijde in het persoonlijke bezit van de drager kan blijven en niet in een bagageruimte hoeft te worden gedeponeerd;

f) de koerier is in het bezit van een door zijn bevoegde veiligheidsautoriteit afgegeven koerierspas op grond waarvan hij gemachtigd is de gespecificeerde gerubriceerde zending te vervoeren.

([11]) De minimumvereisten voor communicatie- en informatiesystemen voor de behandeling van EUCI met rubricering RESTREINT UE/EU RESTRICTED zijn vastgesteld in bijlage III, aanhangsel E.

([12]) Besluit (EU, Euratom) 2019/1962 van de Commissie van 17 oktober 2019 houdende uitvoeringsbepalingen voor de omgang met RESTREINT UE/EU RESTRICTED-informatie (PB L 311 van 2.12.2019, blz. 21).

([13]) Besluit (EU, Euratom) 2019/1961 van de Commissie van 17 oktober 2019 houdende uitvoeringsbepalingen voor de omgang met CONFIDENTIEL UE/EU CONFIDENTIAL- en SECRET UE/EU SECRET-informatie (PB L 311 van 2.12.2019, blz. 1).

4. Voor het vervoer in handbagage door personeel van de begunstigde van als CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gerubriceerde informatie van de ene lidstaat naar de andere, gelden de volgende aanvullende voorschriften:

a) de koerier is verantwoordelijk voor de veilige bewaring van het vervoerde gerubriceerde materiaal totdat het aan de ontvanger wordt overhandigd;

b) in het geval van een beveiligingsinbreuk kan de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de verzender de autoriteiten van het land waar de inbreuk heeft plaatsgevonden, verzoeken een onderzoek in te stellen, verslag uit te brengen over hun bevindingen en, in voorkomend geval, juridische of andere maatregelen te nemen;

c) de koerier is geïnstrueerd over alle veiligheidsverplichtingen die tijdens het vervoer in acht moeten worden genomen en heeft een passende bevestiging ondertekend;

d) de instructies voor de koerier worden aan de koerierspas gehecht;

e) de koerier heeft een beschrijving van de zending en van de route ontvangen;

f) de documenten worden na afloop van de reis (reizen) teruggegeven aan de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van afgifte of worden door de ontvanger bewaard voor controledoeleinden;

g) indien de douane, de immigratiediensten of de grenspolitie de zending willen onderzoeken en inspecteren, mogen zij voldoende delen van de zending openen en controleren om vast te stellen dat deze geen ander materiaal bevat dan het gespecificeerde materiaal;

h) er wordt bij de douaneautoriteiten op aangedrongen om het officiële karakter van de verzendingsdocumenten en van de vergunningsdocumenten die de koerier bij zich heeft, te eerbiedigen.

Indien een zending door de douane wordt geopend, gebeurt dit uit het zicht van niet-gemachtigde personen en, indien mogelijk, in aanwezigheid van de koerier. De koerier verzoekt om herverpakking van de zending en vraagt de autoriteiten die de inspectie uitvoeren, de zending opnieuw te verzegelen en schriftelijk te bevestigen dat deze door hen is geopend.

5. Het vervoer in handbagage door personeel van de begunstigde van als RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gerubriceerde informatie naar een derde land of een internationale organisatie, is onderworpen aan de bepalingen van de informatiebeveiligingsovereenkomst of de administratieve regeling die is gesloten tussen, respectievelijk, de Unie of de Commissie en dat derde land of die internationale organisatie.

HOOFDSTUK 6

BEDRIJFSCONTINUÏTEITSPLANNING

Artikel 16

Rampenplannen en herstelmaatregelen

De subsidieverlenende autoriteit zorgt ervoor dat de gerubriceerde subsidieovereenkomst de begunstigden ertoe verplicht bedrijfsrampenplannen op te stellen teneinde EUCI die in het kader van de uitvoering van de gerubriceerde subsidie wordt behandeld, in noodsituaties te beschermen, en in het kader van de bedrijfscontinuïteitsplanning preventie- en herstelmaatregelen te ontwikkelen om de gevolgen van incidenten in verband met de behandeling en opslag van EUCI tot een minimum te beperken. De begunstigden bevestigen aan de subsidieverlenende autoriteit dat hun bedrijfsrampenplannen zijn ingesteld.

Artikel 17

Inwerkingtreding

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

Gedaan te Brussel, 10 februari 2021.

Voor de Commissie,
namens de voorzitter,
Johannes HAHN
Lid van de Commissie

BIJLAGE I

STANDAARDINFORMATIE IN DE OPROEP

(aan te passen aan de gebruikte oproep)

Beveiliging

Projecten waarbij gerubriceerde EU-informatie gemoeid is, moeten aan een beveiligingscontrole worden onderworpen om financiering mogelijk te maken en kunnen worden onderworpen aan specifieke beveiligingsvoorschriften (nader omschreven in een memorandum over de beveiligingsaspecten, dat aan de subsidieovereenkomst is gehecht).

In deze voorschriften (die vallen onder Besluit (EU, Euratom) 2015/444 van de Commissie ([1]) en/of nationale voorschriften) wordt bijvoorbeeld het volgende bepaald:

— projecten met informatie met rubricering TRES SECRET UE/EU TOP SECRET (of gelijkwaardig) kunnen **NIET** worden gefinancierd;

— gerubriceerde informatie moet worden gemarkeerd overeenkomstig de toepasselijke beveiligingsinstructies in het memorandum over de beveiligingsaspecten;

— informatie met rubriceringsniveaus CONFIDENTIEL UE/EU CONFIDENTIAL of hoger (en RESTREINT UE/EU RESTRICTED indien de nationale voorschriften zulks vereisen) kan:

  — alleen worden gecreëerd of ingezien in bedrijfsruimten met een veiligheidsmachtiging voor een vestiging van de bevoegde nationale veiligheidsautoriteit, conform de nationale voorschriften;

  — alleen worden behandeld in een beveiligde zone die door de bevoegde nationale veiligheidsautoriteit is gehomologeerd;

  — alleen worden ingezien en behandeld door personen met een geldige veiligheidsverklaring voor personeel en een noodzaak tot kennisname ("need-to-know");

— aan het einde van de subsidie moet de gerubriceerde informatie worden teruggegeven of verder worden beschermd conform de toepasselijke voorschriften;

— actietaken waarbij gerubriceerde EU-informatie (EUCI) gemoeid is, mogen alleen worden uitbesteed met voorafgaande schriftelijke toestemming van de subsidieverlenende autoriteit en alleen aan entiteiten die zijn gevestigd in een EU-lidstaat of in een niet-EU-land met een informatiebeveiligingsovereenkomst met de EU (of een administratieve regeling met de Commissie);

— voor de openbaarmaking van EUCI aan derden is de voorafgaande schriftelijke toestemming van de subsidieverlenende autoriteit vereist.

Opgelet: Afhankelijk van het type activiteit is het mogelijk dat de veiligheidsmachtiging voor een vestiging moet worden verstrekt vóór de ondertekening van de subsidie. De subsidieverlenende autoriteit beoordeelt per geval of er behoefte is aan veiligheidsmachtigingen en stelt de datum voor de verstrekking ervan vast tijdens de voorbereiding van de subsidie. Opgelet: wij kunnen **in geen geval** een subsidieovereenkomst ondertekenen wanneer niet ten minste een van de begunstigden van een consortium over een veiligheidsmachtiging voor een vestiging beschikt.

Er kunnen aanvullende beveiligingsaanbevelingen aan de subsidieovereenkomst worden toegevoegd in de vorm van te leveren resultaten op het gebied van beveiliging (*bv. oprichting van een beveiligingsadviesgroep, beperking van de mate van gedetailleerdheid, gebruik van nep-scenario's, het uitsluiten van het gebruik van gerubriceerde informatie enz.*).

De begunstigden moeten ervoor zorgen dat hun projecten niet onderworpen zijn aan nationale veiligheidsvereisten of veiligheidsvereisten van derde landen die van invloed kunnen zijn op de uitvoering van de subsidie of die de toekenning van de subsidie in het gedrang kunnen brengen (*bv. technologische beperkingen, nationale beveiligingsrubricering enz.*). De subsidieverlenende autoriteit moet onmiddellijk in kennis worden gesteld van mogelijke beveiligingsproblemen.

[Aanvullende OPTIE voor kaderpartnerschapsovereenkomsten: Voor kaderpartnerschappen is het mogelijk dat zowel aanvragen voor kaderpartnerschappen als aanvragen voor subsidies aan een beveiligingscontrole moeten worden onderworpen.]

([1]) Zie Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

BIJLAGE II

STANDAARDCLAUSULES IN DE SUBSIDIEOVEREENKOMST

(aan te passen aan de gebruikte subsidieovereenkomst)

13.2. Beveiliging — Gerubriceerde informatie

De partijen moeten gerubriceerde informatie (EU- of nationale informatie) behandelen overeenkomstig de toepasselijke EU- of nationale wetgeving inzake gerubriceerde informatie (met name Besluit (EU, Euratom) 2015/444 van de Commissie ([1]) en de uitvoeringsbepalingen daarvan).

Specifieke veiligheidsvoorschriften zijn (in voorkomend geval) opgenomen in bijlage 5.

BIJLAGE 5

Beveiliging — Gerubriceerde EU-informatie

[OPTIE voor acties met gerubriceerde EU-informatie (standaard): Indien er bij de actie gerubriceerde EU-informatie wordt gebruikt of gecreëerd, moet die informatie, totdat zij wordt gederubriceerd, worden behandeld overeenkomstig de rubriceringsgids en het memorandum over de beveiligingsaspecten, zoals vastgesteld in bijlage 1, en Besluit (EU, Euratom) 2015/444 en de uitvoeringsbepalingen daarvan.

Resultaten die gerubriceerde EU-informatie bevatten, moeten worden ingediend volgens bijzondere procedures die met de subsidieverlenende autoriteit zijn overeengekomen.

Actietaken waarbij gerubriceerde EU-informatie gemoeid is, mogen alleen worden uitbesteed met voorafgaande uitdrukkelijke schriftelijke toestemming van de subsidieverlenende autoriteit en alleen aan entiteiten die zijn gevestigd in een EU-lidstaat of in een niet-EU-land met een informatiebeveiligingsovereenkomst met de EU (of een administratieve regeling met de Commissie).

Gerubriceerde EU-informatie mag niet aan derden (met inbegrip van deelnemers die betrokken zijn bij de uitvoering van de actie) openbaar worden gemaakt zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de subsidieverlenende autoriteit.]

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

BIJLAGE III

[Bijlage IV (bij de ……)]

MEMORANDUM OVER BEVEILIGINGSASPECTEN ([1])

[Model]

([1]) Dit model van het memorandum over de beveiligingsaspecten is van toepassing wanneer de Commissie wordt beschouwd als de bron van de gerubriceerde informatie die voor de uitvoering van de subsidieovereenkomst wordt gecreëerd en behandeld. Wanneer de Commissie niet de bron is van de gerubriceerde informatie die voor de uitvoering van de subsidieovereenkomst wordt gecreëerd en behandeld en wanneer door de aan de subsidie deelnemende lidstaten een specifiek beveiligingskader is opgezet, kunnen er andere modellen van het memorandum over de beveiligingsaspecten van toepassing zijn.

Aanhangsel A

VEILIGHEIDSVEREISTEN

De subsidieverlenende autoriteit moet de onderstaande veiligheidsvereisten opnemen in het memorandum over de beveiligingsaspecten. Sommige clausules zijn mogelijk niet van toepassing op de subsidieovereenkomst. Deze staan tussen vierkante haken.

De lijst van clausules is niet uitputtend. Afhankelijk van de aard van de gerubriceerde subsidie kunnen er extra clausules worden toegevoegd.

ALGEMENE VOORWAARDEN [*NB: van toepassing op alle gerubriceerde subsidieovereenkomsten*]

1. Dit memorandum over de beveiligingsaspecten vormt een integrerend onderdeel van de gerubriceerde subsidieovereenkomst [of van het subcontract] en bevat een beschrijving van de specifieke veiligheidsvereisten voor de subsidieovereenkomst. De niet-inachtneming van deze vereisten kan voldoende reden zijn om de subsidieovereenkomst op te zeggen.

2. Begunstigden van subsidies zijn onderworpen aan alle verplichtingen die zijn vastgesteld in Besluit (EU, Euratom) 2015/444 van de Commissie ([2]) (hierna "Commissiebesluit 2015/444" genoemd) en de uitvoeringsbepalingen daarvan ([3]). Indien de begunstigde van een subsidie een probleem ondervindt bij de toepassing van het toepasselijke rechtskader in een lidstaat, moet hij zich wenden tot de veiligheidsautoriteit van de Commissie en de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit.

3. Gerubriceerde informatie die bij de uitvoering van de subsidieovereenkomst wordt gegenereerd, moet worden gemarkeerd als gerubriceerde EU-informatie (EUCI) met het passende rubriceringsniveau, zoals vastgesteld in de rubriceringsgids in aanhangsel B bij dit memorandum. Afwijkingen van het in de rubriceringsgids vastgestelde rubriceringsniveau zijn alleen toegestaan met schriftelijke toestemming van de subsidieverlenende autoriteit.

4. De rechten die gerelateerd zijn aan de bron van alle EUCI die voor de uitvoering van de gerubriceerde subsidieovereenkomst wordt gecreëerd en behandeld, worden uitgeoefend door de Commissie als subsidieverlenende autoriteit.

5. Zonder schriftelijke toestemming van de subsidieverlenende autoriteit mag de begunstigde of subcontractant informatie die of materiaal dat door de subsidieverlenende autoriteit is verstrekt of namens deze autoriteit is geproduceerd, niet gebruiken voor andere doeleinden dan die van de subsidieovereenkomst.

6. Wanneer een veiligheidsverklaring voor een vestiging vereist is voor de uitvoering van een subsidieovereenkomst, moet de begunstigde de subsidieverlenende autoriteit verzoeken het verzoek om een veiligheidsverklaring voor een vestiging verder te behandelen.

7. De begunstigde moet alle beveiligingsinbreuken in verband met EUCI onderzoeken en deze zo spoedig mogelijk aan de subsidieverlenende autoriteit melden. De begunstigde of subcontractant moet zijn nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit en, wanneer de nationale wet- en regelgeving dit toestaat, de veiligheidsautoriteit van de Commissie onmiddellijk alle gevallen melden waarvan bekend is of waarbij er reden is om te vermoeden dat op grond van de subsidieovereenkomst verstrekte of gegenereerde EUCI verloren is gegaan of aan niet-gemachtigde personen is openbaar gemaakt.

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

([3]) De subsidieverlenende autoriteit moet de referenties invoegen zodra deze uitvoeringsbepalingen zijn aangenomen.

8. Na afloop van de subsidieovereenkomst moet de begunstigde of subcontractant alle EUCI die in zijn bezit is, zo spoedig mogelijk aan de subsidieverlenende autoriteit terugbezorgen. Indien mogelijk kan de begunstigde of subcontractant EUCI vernietigen in plaats van deze terug te bezorgen. Dit moet gebeuren conform de nationale wet- en regelgeving van het land waar de begunstigde is gevestigd, met voorafgaande toestemming van de veiligheidsautoriteit van de Commissie en overeenkomstig de instructies van die veiligheidsautoriteit. EUCI moet op zodanige wijze worden vernietigd dat zij niet geheel of gedeeltelijk kan worden gereconstrueerd.

9. Wanneer de begunstigde of subcontractant gemachtigd is om na de beëindiging of de sluiting van de subsidieovereenkomst EUCI bij zich te houden, moet de EUCI beschermd blijven conform Commissiebesluit 2015/444 en de bijbehorende uitvoeringsbepalingen ([4]).

10. Bij de elektronische behandeling, verwerking en overdracht van EUCI moeten de bepalingen van de hoofdstukken 5 en 6 van Commissiebesluit 2015/444 in acht worden genomen. In deze hoofdstukken is onder meer voorgeschreven dat de communicatie- en informatiesystemen die eigendom zijn van de begunstigde en die worden gebruikt voor de behandeling van EUCI in het kader van de subsidieovereenkomst, moeten worden gehomologeerd ([5]); dat elke elektronische overdracht van EUCI moet worden beschermd door encryptieproducten die zijn goedgekeurd overeenkomstig artikel 36, lid 4, van Commissiebesluit 2015/444 en dat er TEMPEST-beveiligingsmaatregelen moeten worden uitgevoerd overeenkomstig artikel 36, lid 6, van Commissiebesluit 2015/444.

11. De begunstigde of subcontractant moet beschikken over bedrijfsrampenplannen teneinde EUCI die bij de uitvoering van de gerubriceerde subsidieovereenkomst wordt behandeld, in noodsituaties te beschermen, en moet preventie- en herstelmaatregelen ontwikkelen om de gevolgen van incidenten in verband met de behandeling en opslag van EUCI tot een minimum te beperken. De begunstigde of subcontractant moet de subsidieverlenende autoriteit in kennis stellen van zijn bedrijfsrampenplannen.

SUBSIDIEOVEREENKOMSTEN WAARVOOR TOEGANG TOT INFORMATIE MET RUBRICERING RESTREINT UE/EU RESTRICTED IS VEREIST

12. In principe is een veiligheidsverklaring voor personeel niet vereist in het kader van de subsidieovereenkomst ([6]). Informatie of materiaal met rubricering RESTREINT UE/EU RESTRICTED mag echter alleen toegankelijk zijn voor personeel van de begunstigde dat deze informatie nodig heeft om de subsidieovereenkomst uit te voeren (het beginsel "noodzaak tot kennisname") en dat door de veiligheidsagent van de begunstigde is geïnstrueerd over zijn verantwoordelijkheden en over de gevolgen van het compromitteren of schenden van de beveiliging van die informatie, en dat schriftelijk de gevolgen van het niet beschermen van EUCI heeft erkend.

13. Behoudens in het geval van schriftelijke toestemming door de subsidieverlenende autoriteit, mag de begunstigde of subcontractant geen toegang tot informatie of materiaal met rubricering RESTREINT UE/EU RESTRICTED verlenen aan andere entiteiten of personen dan die van zijn personeel die een "noodzaak tot kennisname" hebben.

14. De begunstigde of subcontractant moet de rubriceringsmarkeringen van gerubriceerde informatie die bij de uitvoering van een subsidieovereenkomst wordt gegenereerd of verstrekt, handhaven en mag deze informatie niet derubriceren zonder schriftelijke toestemming van de subsidieverlenende autoriteit.

15. Informatie of materiaal met rubricering RESTREINT UE/EU RESTRICTED moet worden opgeslagen in afgesloten kantoormeubilair wanneer zij of het niet wordt gebruikt. Bij doorvoer moeten documenten in een ondoorzichtige envelop worden vervoerd. De documenten mogen niet uit handen worden gegeven door de drager en mogen onderweg niet worden geopend.

([4]) De subsidieverlenende autoriteit moet de referenties invoegen zodra deze uitvoeringsbepalingen zijn aangenomen.

([5]) De partij die de homologatie wil verkrijgen, moet de subsidieverlenende autoriteit, via de veiligheidsautoriteit van de Commissie en in coördinatie met de desbetreffende nationale veiligheidshomologatieautoriteit, een verklaring van overeenstemming verstrekken.

([6]) Wanneer de begunstigden afkomstig zijn uit lidstaten die veiligheidsverklaringen voor personeel en/of veiligheidsverklaringen voor een vestiging vereisen voor subsidies met rubricering RESTREINT UE/EU RESTRICTED, vermeldt de subsidieverlenende autoriteit in het memorandum over de beveiligingsaspecten deze vereisten inzake veiligheidsverklaringen voor de betrokken begunstigden.

16. De begunstigde of subcontractant mag documenten met rubricering RESTREINT UE/EU RESTRICTED aan de subsidieverlenende autoriteit toezenden via commerciële koeriersdiensten, postdiensten, vervoer in handbagage of elektronische middelen. Daartoe moet de begunstigde of subcontractant de beveiligingsinstructies voor het programma (of project) van de Commissie en/of de uitvoeringsbepalingen van de Commissie inzake industriële beveiliging met betrekking tot gerubriceerde subsidies ([7]) in acht nemen.

17. Indien dit niet langer vereist is, moeten documenten met rubricering RESTREINT UE/EU RESTRICTED op zodanige wijze worden vernietigd dat zij niet geheel of gedeeltelijk kunnen worden gereconstrueerd.

18. De veiligheidshomologatie van het communicatie- en informatiesysteem van de begunstigde waarin EUCI met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld en van de eventuele koppeling daarvan, kan worden gedelegeerd aan de veiligheidsagent van de begunstigde indien de nationale wet- en regelgeving dit toestaat. Wanneer de homologatie aldus wordt gedelegeerd, blijven de nationale veiligheidsautoriteiten, de aangewezen veiligheidsautoriteiten of de veiligheidshomologatieautoriteiten verantwoordelijk voor de bescherming van de door de begunstigde behandelde informatie met rubricering RESTREINT UE/EU RESTRICTED en behouden zij het recht om de door de begunstigde genomen beveiligingsmaatregelen te controleren. Bovendien verstrekt de begunstigde de subsidieverlenende autoriteit en, indien dit is vereist krachtens de nationale wet- en regelgeving, de bevoegde nationale veiligheidshomologatieautoriteit een verklaring van overeenstemming, waarin wordt gecertificeerd dat het communicatie- en informatiesysteem van de begunstigde en de bijbehorende koppelingen zijn gehomologeerd voor de behandeling van EUCI met rubricering RESTREINT UE/EU RESTRICTED.

BEHANDELING VAN INFORMATIE MET RUBRICERING RESTREINT UE/EU RESTRICTED IN COMMUNICATIE- EN INFORMATIESYSTEMEN

19. De minimumvereisten voor communicatie- en informatiesystemen waarin informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld, zijn vastgesteld in aanhangsel E bij dit memorandum over de beveiligingsaspecten.

VOORWAARDEN WAARONDER DE BEGUNSTIGDE EEN BEROEP KAN DOEN OP SUBCONTRACTANTEN

20. De begunstigde moet de toestemming van de subsidieverlenende autoriteit verkrijgen voordat hij een deel van een gerubriceerde subsidieovereenkomst kan uitbesteden.

21. Er mag geen subcontract worden gegund aan een entiteit die is geregistreerd in een niet-EU-land of aan een entiteit die deel uitmaakt van een internationale organisatie, indien dat niet-EU-land of die internationale organisatie geen informatiebeveiligingsovereenkomst met de EU heeft gesloten of geen administratieve regeling met de Commissie heeft getroffen.

22. Wanneer de begunstigde een subcontract heeft toegewezen, zijn de beveiligingsbepalingen van de subsidieovereenkomst van overeenkomstige toepassing op de subcontractant(en) en zijn (hun) personeel. In een dergelijk geval is het de verantwoordelijkheid van de begunstigde om ervoor te zorgen dat alle subcontractanten deze beginselen toepassen in het kader van hun eigen uitbestedingsregelingen. Om een passend veiligheidstoezicht te waarborgen, worden de nationale veiligheidsautoriteiten en/of de aangewezen veiligheidsautoriteiten van de begunstigde en de subcontractant door de veiligheidsautoriteit van de Commissie in kennis gesteld van de toewijzing van alle gelieerde gerubriceerde subcontracten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET. In voorkomend geval wordt aan de nationale veiligheidsautoriteiten en/of de aangewezen veiligheidsautoriteiten van de begunstigde en de subcontractant een kopie van de specifieke beveiligingsbepalingen van de subcontracten verstrekt. De nationale veiligheidsautoriteiten en de aangewezen veiligheidsautoriteiten die kennisgeving verlangen van de beveiligingsbepalingen van gerubriceerde subsidieovereenkomsten van het niveau RESTREINT UE/EU RESTRICTED staan vermeld in de bijlage bij de uitvoeringsbepalingen van de Commissie inzake industriële beveiliging met betrekking tot gerubriceerde subsidieovereenkomsten ([8]).

23. De begunstigde mag geen EUCI vrijgeven aan een subcontractant zonder voorafgaande schriftelijke toestemming van de subsidieverlenende autoriteit. Indien er frequent of systematisch EUCI naar subcontractanten moet worden verstuurd, kan de subsidieverlenende autoriteit haar toestemming geven voor een bepaalde duur (bv. twaalf maanden) of voor de looptijd van het subcontract.

([7]) De subsidieverlenende autoriteit moet de referenties invoegen zodra deze uitvoeringsbepalingen zijn aangenomen.
([8]) De subsidieverlenende autoriteit moet de referenties invoegen zodra deze uitvoeringsbepalingen zijn aangenomen.

BEZOEKEN

Indien de standaardprocedure voor een aanvraag voor een bezoek moet worden toegepast op bezoeken waarbij informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gemoeid is, moet de subsidieverlenende autoriteit de punten 24, 25 en 26 opnemen en punt 27 schrappen. Indien bezoeken waarbij informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET gemoeid is, rechtstreeks tussen de verzendende en de ontvangende instelling worden geregeld, moet de subsidieverlenende autoriteit de punten 25 en 26 schrappen en alleen punt 27 opnemen.

24. Bezoeken die toegang of mogelijke toegang behelzen tot informatie met rubricering RESTREINT UE/EU RESTRICTED, worden rechtstreeks tussen de verzendende en de ontvangende instelling geregeld, zonder dat de in de punten 25, 26 en 27 hieronder beschreven procedure hoeft te worden gevolgd.

[25. Voor bezoeken die toegang of mogelijke toegang behelzen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, geldt de volgende procedure:

a) de veiligheidsagent van de vestiging die de bezoeker stuurt, moet alle relevante onderdelen van het aanvraagformulier voor een bezoek (aanhangsel C) invullen en de aanvraag indienen bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de vestiging;

b) de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de verzendende vestiging moet de veiligheidsverklaring voor personeel van de bezoeker bevestigen voordat de aanvraag voor een bezoek wordt ingediend bij de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging (of de veiligheidsautoriteit van de Commissie in het geval van een bezoek aan de bedrijfsruimten van de subsidieverlenende autoriteit);

c) de veiligheidsagent van de verzendende vestiging ontvangt vervolgens, via zijn nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit, het antwoord van de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit van de ontvangende vestiging (of de veiligheidsautoriteit van de Commissie), die de aanvraag voor een bezoek goedkeurt of afwijst;

d) een aanvraag voor een bezoek wordt geacht te zijn goedgekeurd als er tot vijf werkdagen vóór de datum van het bezoek geen bezwaar wordt gemaakt.]

[26. Alvorens de bezoeker(s) toegang te geven tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, moet de ontvangende vestiging toestemming hebben gekregen van haar nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit.]

[27. Bezoeken die toegang of mogelijke toegang behelzen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, worden rechtstreeks tussen de verzendende en de ontvangende instelling geregeld (een voorbeeld van het formulier dat voor dit doel kan worden gebruikt, is opgenomen in aanhangsel C).]

28. Bezoekers moeten bij aankomst in de ontvangende vestiging hun identiteit bewijzen door een geldige identiteitskaart of een geldig paspoort over te leggen.

29. De ontvangende vestiging moet ervoor zorgen dat er een register wordt bijgehouden van alle bezoekers. Daarin moeten de namen van de bezoekers, de organisatie die zij vertegenwoordigen, de datum waarop de veiligheidsverklaring voor personeel verstrijkt (indien van toepassing), de datum van het bezoek en de naam (namen) van de bezochte persoon (personen) worden geregistreerd. Onverminderd de Europese gegevensbeschermingsregels, moeten deze gegevens worden bewaard gedurende een periode van ten minste vijf jaar of, in voorkomend geval, zoals aangegeven in de nationale wet- en regelgeving.

EVALUATIEBEZOEKEN

30. De veiligheidsautoriteit van de Commissie kan, in samenwerking met de bevoegde nationale veiligheidsautoriteiten of de bevoegde aangewezen veiligheidsautoriteiten, de vestigingen van begunstigden of subcontractanten bezoeken om na te gaan of aan de beveiligingsvereisten voor de behandeling van EUCI is voldaan.

RUBRICERINGSGIDS

31. Een lijst van alle elementen van de subsidieovereenkomst die bij de uitvoering van de subsidieovereenkomst zijn of moeten worden gerubriceerd, de regels daarvoor en de specificaties van de toepasselijke rubriceringsgraden zijn opgenomen in de rubriceringsgids. De rubriceringsgids vormt een integrerend onderdeel van deze subsidieovereenkomst en is opgenomen in aanhangsel B bij deze bijlage.

Aanhangsel B

RUBRICERINGSGIDS

[specifieke tekst aan te passen aan het voorwerp van de subsidieovereenkomst]

Aanhangsel C

AANVRAAG VOOR EEN BEZOEK (MODEL)

GEDETAILLEERDE INSTRUCTIES VOOR HET INVULLEN VAN DE AANVRAAG VOOR EEN BEZOEK

(De aanvraag mag alleen in het Engels worden ingediend)

HEADING	Vink de juiste vakken aan voor het type bezoek en de soort informatie, en geef aan hoeveel vestigingen er bezocht zullen worden en hoeveel bezoekers er zullen komen.
4. **ADMINISTRATIVE DATA**	In te vullen door de aanvragende nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Vermeld de volledige naam en het volledige postadres. Vermeld plaats, land en postcode, indien van toepassing.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Vermeld de volledige naam en het volledige postadres. Vermeld plaats, land, postcode, telex- of faxnummer (indien van toepassing), telefoonnummer en e-mailadres. Geef de naam, het telefoonnummer, het faxnummer en het e-mailadres van uw belangrijkste contactpersoon of de persoon met wie u de afspraak voor het bezoek heeft gemaakt. Opmerkingen: 1) Het vermelden van de juiste postcode is belangrijk omdat een onderneming verschillende vestigingen kan hebben. 2) Bij een handmatige aanvraag kan bijlage 1 worden gebruikt wanneer er twee of meer vestigingen moeten worden bezocht in verband met hetzelfde onderwerp. Wanneer er een bijlage wordt gebruikt, moet in rubriek 3 worden vermeld: “ZIE BIJLAGE 1, AANTAL VESTIGINGEN…” (vermeld het aantal vestigingen).
7. **DATES OF VISIT**	Vermeld de werkelijke datum of periode (datum tot en met datum) van het bezoek in de vorm van “dag-maand-jaar”. Vermeld, in voorkomend geval, een alternatieve datum of periode tussen haakjes.
8. **TYPE OF INITIATIVE**	Geef aan of het bezoek is geïnitieerd door de aanvragende organisatie of vestiging of op uitnodiging van de te bezoeken vestiging.
9. **THE VISIT RELATES TO:**	Vermeld de volledige naam van het project, het contract of de oproep en gebruik daarbij alleen de vaak gebruikte afkortingen.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Geef een korte beschrijving van de reden(en) voor het bezoek. Gebruik geen onverklaarde afkortingen. Opmerkingen: In het geval van herhaalde bezoeken moet in deze rubriek “Herhaalde bezoeken” worden vermeld als de eerste woorden in het gegevenselement (bv. Herhaalde bezoeken voor de bespreking van _____)
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Status SECRET UE/EU SECRET (S-UE/EU-S) of CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), naargelang het geval.

12. **PARTICULARS OF VISITOR**	Opmerking: Wanneer er meer dan twee bezoekers bij het bezoek betrokken zijn, moet bijlage 2 worden gebruikt.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	In deze rubriek moeten de naam, het telefoonnummer, het faxnummer en het e-mailadres van de veiligheidsagent van de aanvragende vestiging worden vermeld.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Dit veld moet worden ingevuld door de certificeringsautoriteit. Opmerkingen voor de certificeringsautoriteit: a. vermeld naam, adres, telefoonnummer, faxnummer en e-mailadres (kan voorgedrukt zijn); b. dit veld moet worden ondertekend en afgestempeld (indien van toepassing).
15. **REQUESTING SECURITY AUTHORITY**	Dit veld moet worden ingevuld door de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit. Opmerking voor de nationale veiligheidsautoriteit/ aangewezen veiligheidsautoriteit: a. vermeld naam, adres, telefoonnummer, faxnummer en e-mailadres (kan voorgedrukt zijn); b. dit veld moet worden ondertekend en afgestempeld (indien van toepassing).

Alle velden moeten worden ingevuld en het formulier moet worden ingediend via intergouvernementele kanalen ([9]).

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**	
Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

([9]) Indien er is overeengekomen dat bezoeken die toegang of mogelijke toegang behelzen tot EUCI met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET rechtstreeks kunnen worden geregeld, kan het ingevulde formulier rechtstreeks bij de veiligheidsagent van de te bezoeken vestiging worden ingediend.

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

EMAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)***

7. **DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____**

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):**

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S) *(Annex 2 to be completed)***

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

EMAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

EMAIL ADDRESS:

SIGNATURE:

STAMP

DATE *(dd/mm/yyyy)*:
_____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

EMAIL ADDRESS:

STAMP

SIGNATURE:

DATE *(dd/mm/yyyy)*:
_____/_____/_____

16. **REMARKS *(Mandatory justification required in the case of an emergency visit)*:**

<Ruimte voor verwijzing naar de toepasselijke wetgeving inzake persoonsgegevens en link naar verplichte informatie voor de betrokkene, bv. hoe artikel 13 van de algemene verordening gegevensbescherming ([10]) ten uitvoer wordt gelegd.>

([10]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

BIJLAGE 1 bij het AANVRAAGFORMULIER VOOR EEN BEZOEK

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: EMAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: EMAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: EMAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: EMAIL: TELEPHONE NO: ***(Continue as required)***

<Ruimte voor verwijzing naar de toepasselijke wetgeving inzake persoonsgegevens en link naar verplichte informatie voor de betrokkene, bv. hoe artikel 13 van de algemene verordening gegevensbescherming ([11]) ten uitvoer wordt gelegd.>

([11]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

BIJLAGE 2 bij het AANVRAAGFORMULIER VOOR EEN BEZOEK

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: ***(Continue as required)***

<Ruimte voor verwijzing naar de toepasselijke wetgeving inzake persoonsgegevens en link naar verplichte informatie voor de betrokkene, bv. hoe artikel 13 van de algemene verordening gegevensbescherming ([12]) ten uitvoer wordt gelegd.>

([12]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

Aanhangsel D

INFORMATIEBLAD VOOR DE VEILIGHEIDSVERKLARING VOOR EEN VESTIGING (MODEL)

1. **INLEIDING**

1.1. Bijgevoegd is een model van een informatieblad voor de veiligheidsverklaring voor een vestiging met het oog op de snelle uitwisseling van informatie tussen de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit, andere bevoegde nationale veiligheidsautoriteiten en de veiligheidsautoriteit van de Commissie (die optreedt namens de subsidieverlenende autoriteiten) met betrekking tot de veiligheidsverklaring voor een vestiging van een vestiging die betrokken is bij de aanvraag en uitvoering van gerubriceerde subsidies of subcontracten.

1.2. Het informatieblad voor de veiligheidsverklaring voor een vestiging is alleen geldig indien het is afgestempeld door de bevoegde nationale veiligheidsautoriteit, de bevoegde aangewezen veiligheidsautoriteit of een andere bevoegde autoriteit.

1.3. Het informatieblad voor de veiligheidsverklaring voor een vestiging is onderverdeeld in een rubriek aanvraag en een rubriek antwoord en kan worden gebruikt voor de bovengenoemde doeleinden of voor andere doeleinden waarvoor voor een bepaalde vestiging de status 'veiligheidsverklaring voor een vestiging' vereist is. De reden voor de aanvraag moet door de aanvragende nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit worden vermeld in veld 7 van de rubriek aanvraag.

1.4. De gegevens in het informatieblad voor de veiligheidsverklaring voor een vestiging zijn normaal gesproken niet gerubriceerd; wanneer er een informatieblad voor de veiligheidsverklaring voor een vestiging tussen de respectieve nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten/Commissie moet worden verzonden, moet dit dus bij voorkeur langs elektronische weg gebeuren.

1.5. De nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten moeten alles in het werk stellen om binnen tien werkdagen te reageren op een aanvraag voor een informatieblad voor de veiligheidsverklaring voor een vestiging.

1.6. Indien er gerubriceerde informatie moet worden overgedragen of een subsidie of subcontract moet worden gegund in het kader van deze garantie, moet de nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit van afgifte daarvan in kennis worden gesteld.

Procedures en instructies voor het gebruik van het informatieblad voor de veiligheidsverklaring voor een vestiging

Deze gedetailleerde instructies zijn bedoeld voor de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit dan wel de subsidieverlenende autoriteit en de veiligheidsautoriteit van de Commissie die het informatieblad aanvult. De aanvraag moet bij voorkeur in hoofdletters worden getypt.

OPSCHRIFT	De aanvrager voegt de volledige naam van de nationale veiligheidsautoriteit/ aangewezen veiligheidsautoriteit en de landnaam in.
1. **TYPE AANVRAAG**	De aanvragende subsidieverlenende autoriteit selecteert het juiste vak voor het type aanvraag voor een informatieblad voor de veiligheidsverklaring voor een vestiging. Vermeld ook het niveau van de aangevraagde veiligheidsverklaring. De volgende afkortingen moeten worden gebruikt: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = communicatie- en informatiesystemen voor de verwerking van gerubriceerde informatie
2. **NADERE GEGEVENS OVER HET ONDERWERP**	De velden 1 tot en met 6 spreken voor zich. In veld 4 moet de gestandaardiseerde tweeletterige landcode worden gebruikt. Veld 5 is facultatief.
3. **REDEN VOOR DE AANVRAAG**	Vermeld de specifieke reden voor de aanvraag, de projectindicatoren en het nummer van de oproep of de subsidie. Specificeer de behoefte aan opslagcapaciteit, het rubriceringsniveau van CIS enz. Alle uiterste datums/vervaldatums/gunningsdatums die gevolgen kunnen hebben voor het invullen van een veiligheidsverklaring voor een vestiging, moeten worden vermeld.

4. **AANVRAGENDE NATIONALE VEILIGHEIDSAUTORITEIT/AANGEWEZEN VEILIGHEIDSAUTORITEIT**	Vermeld de naam van de feitelijke aanvrager (namens de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit), en de datum van de aanvraag in het formaat (dd/mm/jjjj).
5. **RUBRIEK ANTWOORD**	Velden 1-5: selecteer de desbetreffende vakken. Veld 2: indien een veiligheidsverklaring voor een vestiging in behandeling is, is het raadzaam om de aanvrager een indicatie te geven van de behandelingstijd (indien bekend). Veld 6: a) hoewel de validering verschilt van land tot land of zelfs van vestiging tot vestiging, is het raadzaam om de vervaldatum van de veiligheidsverklaring voor een vestiging te vermelden; b) in de gevallen waarin de vervaldatum voor de garantie betreffende de veiligheidsverklaring voor een vestiging onbepaald is, mag dit veld worden doorgehaald; c) ingevolge de respectieve nationale wet- en regelgeving is de aanvrager of de begunstigde of subcontractant verantwoordelijk voor het aanvragen van een verlenging van de veiligheidsverklaring voor een vestiging.
6. **OPMERKINGEN**	Kan worden gebruikt voor aanvullende informatie over de veiligheidsverklaring voor een vestiging, de vestiging of de bovenstaande items.
7. **NATIONALE VEILIGHEIDSAUTORITEIT/AANGEWEZEN VEILIGHEIDSAUTORITEIT VAN AFGIFTE**	Vermeld de naam van de autoriteit van afgifte (namens de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit), en de datum van het antwoord in het formaat (dd/mm/jjjj).

INFORMATIEBLAD VOOR DE VEILIGHEIDSVERKLARING VOOR EEN VESTIGING (MODEL)

Alle velden moeten worden ingevuld en het formulier moet worden ingediend via intergouvernementele kanalen of via kanalen tussen overheidsinstanties en internationale organisaties.

AANVRAAG VOOR EEN GARANTIE BETREFFENDE EEN VEILIGHEIDSVERKLARING VOOR EEN VESTIGING

AAN: _____

(nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit —- landnaam)

Vul, voor zover van toepassing, de onderstaande antwoordvakken in.

[ ] Verstrek een garantie betreffende een veiligheidsverklaring voor een vestiging op het niveau van: [ ] S-UE/EU-S [ ] C-UE/EU-C

voor de hieronder genoemde vestiging,

[ ] met inbegrip van de bescherming van gerubriceerd materiaal/gerubriceerde informatie

[ ] met inbegrip van communicatie- en informatiesystemen (CIS) voor de verwerking van gerubriceerde informatie

[ ] Initieer, rechtstreeks of op verzoek van een begunstigde of subcontractant, het proces om een veiligheidsverklaring voor een vestiging te verkrijgen tot en met het niveau van ....., en met ..... niveau van bescherming en ..... niveau van CIS, indien de vestiging deze beschermingsniveaus momenteel niet kan bieden.

Bevestig de juistheid van de onderstaande gegevens over de vestiging en breng zo nodig correcties/aanvullingen aan.

1. Volledige naam van de vestiging:	Correcties/Aanvullingen:
.....	.....
2. Volledig adres van de vestiging:	
.....	.....
3. Postadres (indien verschillend van 2)	
.....	.....
4. Postcode/stad/land	
.....	.....
5. Naam van de veiligheidsagent	
.....	
.....	
6. Telefoon/Fax/E-mail van de veiligheidsagent	
.....	.....

7. Deze aanvraag wordt gedaan om de volgende reden(en): (verstrek nadere gegevens over de precontractuele fase (selectie van voorstellen), de subsidie of het subcontract, het programma/project enz.)

.....

Aanvragende nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit/subsidieverlenende autoriteit: Naam: .....

Datum: (dd/mm/jjjj) .....

ANTWOORD (binnen tien werkdagen)

Hierbij wordt gecertificeerd dat:

1. [ ] de bovengenoemde vestiging in het bezit is van een veiligheidsverklaring voor een vestiging tot en met het niveau [ ] S-UE/EU-S

   [ ] C-UE/EU-C

2. de bovengenoemde vestiging in staat is om gerubriceerde informatie/gerubriceerd materiaal te beschermen:

   [ ] ja, niveau: ..... [ ] neen

3. de bovengenoemde vestiging beschikt over een gehomologeerd/goedgekeurd CIS:

   [ ] ja, niveau: ..... [ ] neen

4. [ ] met betrekking tot bovengenoemde aanvraag het proces om een veiligheidsverklaring voor een vestiging te verkrijgen, is geïnitieerd. U zal ervan in kennis worden gesteld wanneer de veiligheidsverklaring voor een vestiging is verleend of is geweigerd;

5. [ ] de bovengenoemde vestiging niet in het bezit is van een veiligheidsverklaring voor een vestiging;

6. deze garantie betreffende een veiligheidsverklaring voor een vestiging verstrijkt op ..... (*dd/mm/jjjj*) of zoals aangegeven door de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit. In het geval van eerdere ongeldigverklaring of wijziging van de bovenstaande informatie, zal u hiervan in kennis worden gesteld.

7. Opmerkingen:
   .....

Nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit van afgifte Naam: .....

Datum:(dd/mm/jjjj) .....

<Ruimte voor verwijzing naar de toepasselijke wetgeving inzake persoonsgegevens en link naar verplichte informatie voor de betrokkene, bv. hoe artikel 13 van de algemene verordening gegevensbescherming ([13]) ten uitvoer wordt gelegd.>

([13]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

Aanhangsel E

Minimumvereisten voor de bescherming van als RESTREINT UE/EU RESTRICTED gerubriceerde EUCI in elektronische vorm die wordt behandeld in het communicatie- en informatiesysteem van de begunstigde

Algemeen

1. De begunstigde moet ervoor zorgen dat de bescherming van informatie met rubricering RESTREINT UE/EU RESTRICTED voldoet aan de minimale veiligheidsvereisten van deze beveiligingsclausules en aan alle andere aanvullende vereisten die door de subsidieverlenende autoriteit of, in voorkomend geval, de nationale veiligheidsautoriteit of de aangewezen veiligheidsautoriteit worden aanbevolen.

2. Het is de verantwoordelijkheid van de begunstigde om de in dit document vastgestelde veiligheidsvereisten ten uitvoer te leggen.

3. In dit document wordt onder een communicatie- en informatiesysteem verstaan alle apparatuur die wordt gebruikt voor de behandeling, opslag en overdracht van EUCI, met inbegrip van werkstations, printers, kopieerapparaten, faxapparaten, servers, netwerkbeheersystemen, netwerk- en communicatiecontrollers, laptops, notebooks, tablets, smartphones en verwijderbare opslagapparatuur zoals USB-sticks, cd's, SD-kaarten enz.

4. Speciale apparatuur, zoals encryptieproducten, moet worden beschermd conform specifieke operationele beveiligingsprocedures.

5. De begunstigde moet een structuur opzetten voor het beveiligingsbeheer van het communicatie- en informatiesysteem waarin informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld, en een veiligheidsagent aanstellen voor de betrokken vestiging.

6. Het gebruik van IT-oplossingen (hardware, software of diensten) die privé-eigendom zijn van personeel van de begunstigde voor de opslag of verwerking van informatie met rubricering RESTREINT UE/EU RESTRICTED, is niet toegestaan.

7. De homologatie van het communicatie- en informatiesysteem van de begunstigde waarin informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld, moet worden goedgekeurd door de veiligheidshomologatieautoriteit van de betrokken lidstaat of worden gedelegeerd aan de veiligheidsagent van de begunstigde, overeenkomstig de nationale wet- en regelgeving.

8. Alleen informatie met rubricering RESTREINT UE/EU RESTRICTED die met goedgekeurde encryptieproducten is versleuteld, mag worden behandeld, opgeslagen of overgedragen (per draad of draadloos), net als alle andere niet-gerubriceerde informatie in het kader van de subsidieovereenkomst. Dergelijke encryptieproducten moeten door de EU of een lidstaat worden goedgekeurd.

9. Externe vestigingen die betrokken zijn bij onderhouds-/reparatiewerkzaamheden, moeten contractueel verplicht zijn te voldoen aan de toepasselijke bepalingen inzake de behandeling van informatie met rubricering RESTREINT UE/EU RESTRICTED, zoals in dit document is vastgesteld.

10. Op verzoek van de subsidieverlenende autoriteit of de betrokken nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit of de veiligheidshomologatieautoriteit moet de begunstigde aantonen dat hij de beveiligingsclausules van de subsidieovereenkomst in acht neemt. Indien er tevens wordt verzocht om een audit en een inspectie van de processen en vestigingen van de begunstigde teneinde de inachtneming van deze vereisten te controleren, moeten de begunstigden toestaan dat vertegenwoordigers van de subsidieverlenende autoriteit, de nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit en/of de veiligheidshomologatieautoriteit of de betrokken veiligheidsautoriteit van de EU een dergelijke audit en inspectie uitvoeren.

Fysieke beveiliging

11. Ruimten waarin communicatie- en informatiesystemen worden gebruikt om informatie met rubricering RESTREINT UE/EU RESTRICTED weer te geven, op te slaan, te verwerken of over te dragen of ruimten waarin er zich servers, netwerkbeheersystemen, netwerk- en communicatiecontrollers voor dergelijke communicatie- en informatiesystemen bevinden, moeten worden afgebakend als afzonderlijke en gecontroleerde ruimten met een passend toegangscontrolesysteem. De toegang tot deze afzonderlijke en gecontroleerde ruimten moet worden beperkt tot personen met een specifieke machtiging. Onverminderd punt 8 moet de in punt 3 beschreven apparatuur in dergelijke afzonderlijke en gecontroleerde ruimten worden opgeslagen.

12. Er moeten beveiligingsmechanismen en/of -procedures worden toegepast om de invoering of de aansluiting van verwijderbare digitale opslagdragers (zoals USB-sticks, apparaten voor massaopslag of CD-RW's) op onderdelen van het communicatie- en informatiesysteem te regelen.

Toegang tot het communicatie- en informatiesysteem

13. Toegang tot het communicatie- en informatiesysteem van een begunstigde waarin EUCI wordt behandeld, wordt verleend op grond van een strikte "noodzaak tot kennisname" en middels een machtiging voor het personeel.

14. Voor alle communicatie- en informatiesystemen moeten er bijgewerkte lijsten van gemachtigde gebruikers zijn. Alle gebruikers moeten aan het begin van elke verwerkingssessie worden geauthenticeerd.

15. Wachtwoorden, die deel uitmaken van de meeste identificatie- en authenticatiebeveiligingsmaatregelen, moeten minstens negen tekens lang zijn en moeten numerieke en "speciale" tekens (indien dit mogelijk is in het systeem) bevatten, alsmede alfabetische tekens. Wachtwoorden moeten minstens om de 180 dagen worden gewijzigd. Zij moeten zo spoedig mogelijk worden gewijzigd indien zij gecompromitteerd zijn of aan een niet-gemachtigde persoon zijn bekendgemaakt, of indien het vermoeden bestaat dat dit is gebeurd.

16. Voor alle communicatie- en informatiesystemen moeten er interne toegangscontroles zijn om te voorkomen dat niet-gemachtigde gebruikers toegang krijgen tot informatie met rubricering RESTREINT UE/EU RESTRICTED of deze informatie kunnen wijzigen en dat niet-gemachtigde gebruikers het systeem en de beveiligingscontroles kunnen wijzigen. Gebruikers moeten automatisch worden uitgelogd uit het communicatie- en informatiesysteem wanneer hun terminals gedurende een vooraf bepaalde periode inactief zijn, of het communicatie- en informatiesysteem moet een met een wachtwoord beveiligde screensaver activeren na 15 minuten inactiviteit.

17. Elke gebruiker van het communicatie- en informatiesysteem moet een unieke gebruikersaccount en -naam krijgen. Gebruikersaccounts moeten automatisch worden geblokkeerd na ten minste vijf opeenvolgende mislukte inlogpogingen.

18. Alle gebruikers van het communicatie- en informatiesysteem moeten worden gewezen op hun verantwoordelijkheden en op de procedures die moeten worden gevolgd om informatie met rubricering RESTREINT UE/EU RESTRICTED in het communicatie- en informatiesysteem te beschermen. Deze verantwoordelijkheden en te volgen procedures moeten schriftelijk worden vastgelegd en door de gebruikers schriftelijk worden bevestigd.

19. Operationele beveiligingsprocedures moeten beschikbaar zijn voor de gebruikers en beheerders en moeten beschrijvingen van de beveiligingsfuncties en de bijbehorende lijst van taken, instructies en plannen bevatten.

Logboeken, audits en respons op incidenten

20. Elke toegang tot het communicatie- en informatiesysteem moet worden geregistreerd.

21. De volgende gebeurtenissen moeten worden geregistreerd:

    a) alle succesvolle of mislukte inlogpogingen;

    b) het uitloggen (eventueel met inbegrip van een time-out);

    c) het aanmaken, verwijderen of wijzigen van toegangsrechten en -voorrechten;

    d) het aanmaken, verwijderen of wijzigen van wachtwoorden.

22. Voor alle hierboven genoemde gebeurtenissen moet ten minste de volgende informatie worden gerapporteerd:

    a) soort gebeurtenis;

    b) gebruikersnaam;

    c) datum en tijd;

    d) identificatienummer van het apparaat.

23. Logboeken moeten voor een veiligheidsagent een hulpmiddel zijn bij het onderzoek van mogelijke veiligheidsincidenten. Zij kunnen ook worden gebruikt ter ondersteuning van gerechtelijke onderzoeken in het geval van een veiligheidsincident. Alle veiligheidsregisters moeten regelmatig worden gecontroleerd om mogelijke veiligheidsincidenten te identificeren. Logboeken moeten worden beschermd tegen ongeoorloofde vernietiging of wijziging.

24. De begunstigde moet beschikken over een vaste responsstrategie voor het afhandelen van veiligheidsincidenten. Gebruikers en beheerders moeten worden geïnstrueerd hoe zij op incidenten moeten reageren, hoe zij incidenten moeten melden en wat zij moeten doen in een noodsituatie.

25. De compromittering of vermoedelijke compromittering van informatie met rubricering RESTREINT UE/EU RESTRICTED moet aan de subsidieverlenende autoriteit worden gemeld. De melding moet een beschrijving bevatten van de betrokken informatie en een beschrijving van de omstandigheden van de compromittering of vermoedelijke compromittering. Alle gebruikers van het communicatie- en informatiesysteem moeten op de hoogte worden gebracht van de wijze waarop zij elk daadwerkelijk of vermoedelijk veiligheidsincident aan de veiligheidsagent kunnen melden.

Netwerken en koppeling

26. Wanneer een communicatie- en informatiesysteem van de begunstigde waarin informatie met rubricering RESTREINT UE/EU RESTRICTED wordt behandeld, gekoppeld is aan een communicatie- en informatiesysteem dat niet is gehomologeerd, is er sprake van een aanzienlijke verhoging van de dreiging voor de beveiliging van het communicatie- en informatiesysteem en van de informatie met rubricering RESTREINT UE/EU RESTRICTED die in dat systeem wordt behandeld. Dit omvat koppelingen via het internet en andere openbare of particuliere communicatie- en informatiesystemen, zoals andere communicatie- en informatiesystemen die eigendom zijn van de begunstigde of subcontractant. In dat geval moet de begunstigde een risicobeoordeling uitvoeren om te bepalen welke extra veiligheidsvereisten er in het kader van de veiligheidshomologatieprocedure moeten worden nageleefd. De begunstigde verstrekt de subsidieverlenende autoriteit en, indien dit is vereist krachtens de nationale wet- en regelgeving, de bevoegde veiligheidshomologatieautoriteit een verklaring van overeenstemming, waarin wordt gecertificeerd dat het communicatie- en informatiesysteem van de begunstigde en de bijbehorende koppelingen zijn gehomologeerd voor de behandeling van EUCI met rubricering RESTREINT UE/EU RESTRICTED.

27. Toegang op afstand tot lokale netwerkdiensten vanuit andere systemen (bv. toegang op afstand tot e-mail en systeemondersteuning op afstand) is verboden, tenzij er bijzondere beveiligingsmaatregelen worden toegepast en worden goedgekeurd door de subsidieverlenende autoriteit en, indien dit is vereist krachtens de nationale wet- en regelgeving, door de bevoegde veiligheidshomologatieautoriteit.

Configuratiebeheer

28. Er moet een gedetailleerde hard- en softwareconfiguratie, zoals weergegeven in de homologatie-/goedkeuringsdocumentatie (met inbegrip van systeem- en netwerkdiagrammen), beschikbaar zijn en deze moet regelmatig worden bijgewerkt.

29. De veiligheidsagent van de begunstigde moet de hard- en softwareconfiguratie controleren om zich ervan te vergewissen dat er geen ongeautoriseerde hard- of software is geïnstalleerd.

30. Wijzigingen in de configuratie van het communicatie- en informatiesysteem van de begunstigde moeten worden beoordeeld op hun gevolgen voor de veiligheid en moeten worden goedgekeurd door de veiligheidsagent en, indien dit is vereist krachtens de nationale wet- en regelgeving, door de veiligheidshomologatieautoriteit.

31. Het systeem moet ten minste eenmaal per kwartaal worden gescand op kwetsbaarheden in de beveiliging. Software voor de opsporing van malware moet worden geïnstalleerd en up-to-date worden gehouden. Indien mogelijk moet er voor deze software een nationale of erkende internationale goedkeuring zijn of anders moet deze software in overeenstemming zijn met een algemeen aanvaarde industrienorm.

32. De begunstigde moet een bedrijfscontinuïteitsplan ontwikkelen. Er moeten back-upprocedures worden vastgesteld voor de volgende aspecten:

    a) de frequentie van de back-ups;

    b) de voorschriften voor opslag ter plaatse (brandwerende containers) of buiten het bedrijfsterrein;

    c) controle op de geautoriseerde toegang tot back-ups.

Cleaning en vernietiging

33. Communicatie- en informatiesystemen of gegevensopslagdragers waarop op enig moment informatie met rubricering RESTREINT UE/EU RESTRICTED is bewaard, moeten op de volgende wijze worden gecleand voordat ze worden afgevoerd:

    a) flashgeheugens (bv. USB-sticks, SD-kaarten, solidstateschijven en hybride harde schijven) moeten ten minste drie keer worden overschreven en vervolgens moet worden gecontroleerd of de oorspronkelijke inhoud niet kan worden gerecupereerd, of moeten worden gewist met behulp van goedgekeurde wissoftware;

    b) magnetische dragers (bv. harde schijven) moeten worden overschreven of gedemagnetiseerd;

    c) optische dragers (bv. cd's en dvd's) moeten worden versnipperd of gedesintegreerd;

    d) voor alle andere opslagdragers moet de subsidieverlenende autoriteit of, in voorkomend geval, de nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit of de veiligheidshomologatieautoriteit worden geraadpleegd over de in acht te nemen veiligheidsvereisten.

34. Informatie met rubricering RESTREINT UE/EU RESTRICTED moet worden gecleand op alle gegevensdragers voordat deze worden verstrekt aan entiteiten die niet gemachtigd zijn om toegang te krijgen tot informatie met rubricering RESTREINT UE/EU RESTRICTED (bv. voor onderhoudswerkzaamheden).

BIJLAGE IV

Veiligheidsverklaring voor een vestiging en veiligheidsverklaring voor personeel voor begunstigden of subcontractanten die te maken krijgen met informatie met rubricering RESTREINT UE/EU RESTRICTED en nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten die kennisgeving verlangen van gerubriceerde subsidieovereenkomsten van het niveau RESTREINT UE/EU RESTRICTED ([1])

Lidstaat	Veiligheidsverklaring voor een vestiging		Kennisgeving aan de nationale veiligheidsautoriteit en/of de aangewezen veiligheidsautoriteit van subsidieovereenkomsten of subcontracten waarbij informatie met rubricering RESTREINT UE/EU RESTRICTED gemoeid is		Veiligheidsverklaring voor personeel	
	JA	NEEN	JA	NEEN	JA	NEEN
België		**X**		**X**		**X**
Bulgarije		**X**		**X**		**X**
Tsjechië		**X**		**X**		**X**
Denemarken	**X**		**X**		**X**	
Duitsland		**X**		**X**		**X**
Estland	**X**		**X**			**X**
Ierland		**X**		**X**		**X**
Griekenland	**X**			**X**	**X**	
Spanje		**X**	**X**			**X**
Frankrijk		**X**		**X**		**X**
Kroatië		**X**	**X**			**X**
Italië		**X**	**X**			**X**
Cyprus		**X**	**X**			**X**
Letland		**X**		**X**		**X**
Litouwen	**X**		**X**			**X**
Luxemburg	**X**		**X**		**X**	
Hongarije		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nederland	**X** (alleen voor defensiegerelateerde subsidieovereenkomsten en subcontracten)		**X** (alleen voor defensiegerelateerde subsidieovereenkomsten en subcontracten)			**X**
Oostenrijk		**X**		**X**		**X**
Polen		**X**		**X**		**X**

([1]) Deze nationale voorschriften inzake een veiligheidsverklaring voor een vestiging/veiligheidsverklaring voor personeel en inzake kennisgeving voor subsidieovereenkomsten waarbij informatie met rubricering RESTREINT UE/EU RESTRICTED gemoeid is, mogen geen extra verplichtingen opleggen aan andere lidstaten of aan begunstigden en subcontractanten die onder hun bevoegdheid vallen.
NB: De kennisgeving van subsidieovereenkomsten waarbij informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gemoeid is, is verplicht.

Portugal		**X**		**X**		**X**
Roemenië		**X**		**X**		**X**
Slovenië	**X**		**X**			**X**
Slowakije	**X**		**X**			**X**
Finland		**X**		**X**		**X**
Zweden		**X**		**X**		**X**

BIJLAGE V

LIJST VAN DIENSTEN VAN NATIONALE VEILIGHEIDSAUTORITEITEN/AANGEWEZEN VEILIGHEIDSAUTORITEITEN DIE VERANTWOORDELIJK ZIJN VOOR DE PROCEDURES INZAKE INDUSTRIËLE BEVEILIGING

BELGIË

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels

Tel. +32 25014542 (Secretariat)

Fax +32 25014596

E-mail: nvo-ans@diplobel.fed.be

BULGARIJE

1. State Commission on Information Security — National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel. +359 29835775
   Fax +359 29873750
   E-mail: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel. +359 29227002
   Fax +359 29885211
   E-mail: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel. +359 29813221
   Fax +359 29862706
   E-mail: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel. +359 29824971
   Fax +359 29461339
   E-mail: dato@dato.bg

(De bovengenoemde bevoegde autoriteiten passen de doorlichtingsprocedures toe voor de afgifte van veiligheidsverklaringen voor een vestiging aan rechtspersonen die een gerubriceerd contract willen sluiten, en voor de afgifte van veiligheidsverklaringen voor personeel aan personen die een gerubriceerd contract uitvoeren ten behoeve van deze autoriteiten)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.

   1407 Sofia

   Tel. +359 28147109

   Fax +359 29632188, +359 28147441

   E-mail: dans@dans.bg

(De bovengenoemde veiligheidsdienst past de doorlichtingsprocedures toe voor de afgifte van veiligheidsverklaringen voor een vestiging en veiligheidsverklaringen voor personeel aan alle andere rechtspersonen en personen in het land die een gerubriceerd contract of een gerubriceerde subsidieovereenkomst willen sluiten of een gerubriceerd contract of een gerubriceerde subsidieovereenkomst uitvoeren)

TSJECHIË

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56

Tel. +420 257283129

E-mail: sbr@nbu.cz

DENEMARKEN

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Tel. +45 33148888

   Fax +45 33430190

2. Forsvarets Efterretningstjeneste
   (Danish Defence Intelligence Service)
   Kastellet 30
   2100 Copenhagen Ø

   Tel. +45 33325566

   Fax +45 33931320

DUITSLAND

1. Voor aangelegenheden met betrekking tot het industriële veiligheidsbeleid, veiligheidsverklaringen voor een vestiging, vervoerplannen (behalve voor encryptieproducten/CCI):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division — RS3

   Villemombler Str. 76

   53123 Bonn

   Tel. +49 228996154028

   Fax +49 228996152676

   E-mail: dsagermany-rs3@bmwi.bund.de (office email address)

2. Aanvragen voor standaardbezoeken van/aan Duitse bedrijven:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division — RS2
Villemombler Str. 76
53123 Bonn

Tel. +49 228996152401

Fax +49 228996152603

E-mail: rs2-international@bmwi.bund.de (office email address)

3. Vervoerplannen voor encryptiemateriaal:

Federal Office for Information Security (BSI)
National Distribution Agency / NDA-EU DEU
Mainzer Str. 84
53179 Bonn

Tel. +49 2289995826052

Fax +49 228991095826052

E-mail: NDAEU@bsi.bund.de

ESTLAND

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn

Tel. +372 6939211

Fax +372 6935001

E-mail: nsa@fis.gov.ee

IERLAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45

Tel. +353 14082724

E-mail: nsa@dfa.ie

GRIEKENLAND

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens

Tel. +30 2106572022, +30 2106572178

Fax +30 2106527612

E-mail: daa.industrial@hndgs.mil.gr

SPANJE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel. +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

E-mail: nsa-sp@areatec.com

Voor informatie over gerubriceerde programma's: programas.ons@areatec.com

Voor aangelegenheden met betrekking tot veiligheidsverklaringen voor personeel: hps.ons@areatec.com

Voor vervoerplannen en internationale bezoeken: sp-ivtco@areatec.com

FRANKRIJK

National Security Authority (NSA) (voor beleid en tenuitvoerlegging op andere gebieden dan de defensie-industrie)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel. +33 171758193

Fax +33 171758200

E-mail: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (voor tenuitvoerlegging in de defensie-industrie)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15

Tel. +33 988670421

E_mail: voor formulieren en uitgaande aanvragen voor een bezoek: dga-ssdi.ai.fct@intradef.gouv.fr

voor inkomende aanvragen voor een bezoek: dga-ssdi.visit.fct@intradef.gouv.fr

KROATIË

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb

Tel. +385 14681222

Fax +385 14686049

E-mail: NSACroatia@uvns.hr

ITALIË

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel. +39 0661174266

Fax +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Tel. +357 22807569, +357 22807764

Fax +357 22302351

E-mail: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Tel. +357 22807569, +357 22807764

Fax +357 22302351

E-mail: cynsa@mod.gov.cy

LETLAND

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001

Tel. +371 67025418, +371 67025463

Fax +371 67025454

E-mail: ndi@sab.gov.lv, ndi@zd.gov.lv

LITOUWEN

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Pilaitės pr. 19
LT-06264 Vilnius

Tel. +370 70666128

E-mail: nsa@vsd.lt

LUXEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxemburg

Tel. +352 24782210

E-mail: ans@me.etat.lu

HONGARIJE

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 13911862

Fax +36 13911889

E-mail: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010

Tel.+356 23952000

Fax +356 21242406

E-mail: certification@mccaa.org.mt

NEDERLAND

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA The Hague

   Tel. +31 703204400

   Fax +31 703200733

   E-mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES The Hague

   Tel. +31 704419407

   Fax +31 703459189

   E-mail: indussec@mindef.nl

OOSTENRIJK

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tel. +43 153115202594

   E-mail: isk@bka.gv.at

2. DSA in the military sphere:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   E-mail: abwa@bmlvs.gv.at

POLEN

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw

Tel. +48 225857944

Fax +48 225857443

E-mail: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nr. 69
1300-342 Lisbon

Tel. +351 213031710

Fax +351 213031711

E-mail: sind@gns.gov.pt, franco@gns.gov.pt

ROEMENIË

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS
Romanian NSA — ORNISS — National Registry Office for Classified Information
4th Mures Street
012275 Bucharest

Tel. +40 212075115

Fax +40 212245830

E-mail: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIË

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel. +386 14781390

Fax +386 14781399

E-mail: gp.uvtp@gov.si

SLOWAKIJE

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Tel. +421 268691111

Fax +421 268691700

E-mail: podatelna@nbu.gov.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

E-mail: NSA@formin.fi

ZWEDEN

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK / NSA
   SE-103 39 Stockholm
   Tel. +46 84051000
   Fax +46 87231176
   E-mail: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel. +46 87824000
   Fax +46 87826900
   E-mail: security@fmv.se