

Publicatieblad

van de Europese Unie

C 126



Uitgave
in de Nederlandse taal

Mededelingen en bekendmakingen

61e jaargang

10 april 2018

Inhoud

IV *Informatie*

INFORMATIE AFKOMSTIG VAN DE INSTELLINGEN, ORGANEN EN INSTANTIES VAN DE EUROPESE UNIE

2018/C 126/01

Besluit van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 19 september 2017 betreffende de beveiligingsvoorschriften voor de Europese Dienst voor extern optreden — ADMIN(2017) 10

1

NL

IV

*(Informatie)*INFORMATIE AFKOMSTIG VAN DE INSTELLINGEN, ORGANEN EN
INSTANTIES VAN DE EUROPESE UNIE

EUROPESE DIENST VOOR EXTERN OPTREDEN

**Besluit van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid
van 19 september 2017 betreffende de beveiligingsvoorschriften voor de Europese Dienst voor
extern optreden**

ADMIN(2017) 10

(2018/C 126/01)

DE HOGE VERTEGENWOORDIGER VAN DE UNIE VOOR BUITENLANDSE ZAKEN EN VEILIGHEIDSBELEID,

Gezien Besluit 2010/427/EU van de Raad van 26 juli 2010 tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden ⁽¹⁾ (hierna „EDEO” genoemd),

Gezien het advies van het comité bedoeld in artikel 9, lid 6, van het besluit van de hoge vertegenwoordiger van 15 juni 2011 betreffende de beveiligingsvoorschriften voor de Europese Dienst voor extern optreden ⁽²⁾,

Overwegende hetgeen volgt:

- (1) De EDEO dient als functioneel autonoom orgaan van de Europese Unie (hierna „EU” genoemd) te beschikken over beveiligingsvoorschriften als bedoeld in artikel 10, lid 1, van Besluit 2010/427/EU.
- (2) De hoge vertegenwoordiger van de Unie voor Buitenlandse Zaken en Veiligheidsbeleid (hierna „de hoge vertegenwoordiger” genoemd) dient beveiligingsvoorschriften voor de EDEO vast te stellen die betrekking hebben op alle aspecten van beveiliging die met de werking van de EDEO verband houden, zodat de EDEO de risico's voor het onder zijn verantwoordelijkheid geplaatste personeel, zijn materiële activa, zijn informatie en zijn bezoekers doeltreffend kan beheersen en zijn zorgplicht en andere verplichtingen in dit verband kan vervullen.
- (3) Met name dient voor het onder de verantwoordelijkheid van de EDEO geplaatste personeel en voor de materiële activa, met inbegrip van communicatie- en informatiesystemen, de informatie en de bezoekers van de EDEO een beschermingsniveau te worden gegarandeerd dat in overeenstemming is met de beste praktijken bij de Raad van de Europese Unie, de Europese Commissie, de lidstaten en, waar van toepassing, internationale organisaties.
- (4) De beveiligingsvoorschriften voor de EDEO dienen bij te dragen tot een coherenter algemeen kader binnen de EU voor de bescherming van gerubriceerde EU-informatie, op basis van en zo veel mogelijk in overeenstemming met de beveiligingsvoorschriften van de Raad van de Europese Unie (hierna „de Raad” genoemd) en de beveiligingsbepalingen van de Europese Commissie (hierna „de Commissie” genoemd).
- (5) De EDEO, de Raad en de Commissie zijn gehouden gelijkwaardige beveiligingsnormen toe te passen voor de bescherming van gerubriceerde EU-informatie.
- (6) Dit besluit laat de artikelen 15 en 16 van het Verdrag betreffende de werking van de Europese Unie (hierna „VWEU” genoemd) en de instrumenten ter uitvoering daarvan onverlet.

⁽¹⁾ PB L 201 van 3.8.2010, blz. 30.

⁽²⁾ PB C 304 van 15.10.2011, blz. 7.

- (7) De organisatie van de beveiliging in de EDEO en de toewijzing van beveiligingstaken aan de structuren van de EDEO dienen te worden vastgesteld.
- (8) De hoge vertegenwoordiger dient waar nodig gebruik te maken van relevante deskundigheid bij de lidstaten, het secretariaat-generaal van de Raad en de Commissie.
- (9) De hoge vertegenwoordiger dient alle passende maatregelen te nemen die noodzakelijk zijn voor de tenuitvoerlegging van deze voorschriften, met de steun van de lidstaten, het secretariaat-generaal van de Raad en de Commissie.
- (10) De secretaris-generaal van de EDEO is de veiligheidsautoriteit van de EDEO, en in artikel 1 van Besluit ADMIN (2015)³⁴ van 14 september 2015 van de secretaris-generaal van de EDEO wordt bepaald dat, zoals bepaald in de beveiligingsvoorschriften van de EDEO, de veiligheidsfuncties van de veiligheidsautoriteit worden uitgeoefend door de directeur-generaal begroting en administratie,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Doel en werkingssfeer

Bij dit besluit worden de voorschriften voor de beveiliging van de Europese Dienst voor extern optreden (hierna „beveiligingsvoorschriften van de EDEO” genoemd) vastgesteld.

Overeenkomstig artikel 10, lid 1, van Besluit 2010/427/EU van de Raad van 26 juli 2010 tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden gelden deze voorschriften voor alle personeelsleden van de EDEO en van de delegaties van de Unie, ongeacht hun administratieve status of herkomst, en wordt bij dit besluit het algemene regelgevingskader vastgesteld voor het doeltreffende beheer van de risico's voor het onder de verantwoordelijkheid van de EDEO geplaatste personeel, als bedoeld in artikel 2, en voor de locaties, de materiële activa, de informatie en de bezoekers van de EDEO.

Artikel 2

Definities

In dit besluit wordt verstaan onder:

- a) „personeel/personeelsleden van de EDEO”: ambtenaren en andere personeelsleden van de EDEO, met inbegrip van personeelsleden van de diplomatieke diensten van de lidstaten die zijn aangesteld als tijdelijke functionaris en gedetacheerde nationale deskundigen, zoals bedoeld in artikel 6 van Besluit 2010/427/EU van de Raad van 26 juli 2010 tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden;
- b) „onder de verantwoordelijkheid van de EDEO geplaatst personeel”: personeel van de EDEO op het hoofdkantoor en in de delegaties van de Unie, en alle andere personeelsleden in de delegaties van de Unie, ongeacht hun administratieve status of herkomst, alsmede in de context van dit besluit de hoge vertegenwoordiger en in voorkomend geval andere personeelsleden die in het hoofdkantoor van de EDEO verblijven;
- c) „personen te hunnen laste”: gezinsleden van onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden in delegaties van de Unie die deel uitmaken van hun huishouden en als zodanig zijn aangemeld bij het Ministerie van Buitenlandse Zaken van de ontvangende staat;
- d) „locaties van de EDEO”: alle vestigingen van de EDEO, waaronder gebouwen, kantoren, ruimten en andere zones, alsmede zones waar communicatie- en informatiesystemen zijn ondergebracht (met inbegrip van die waar gerubriceerde EU-informatie wordt verwerkt), waar de EDEO permanente of tijdelijke activiteiten ontplooit;
- e) „veiligheidsbelangen van de EDEO”: onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden, personen te hunnen laste, locaties, materiële activa, waaronder communicatie- en informatiesystemen, informatie en bezoekers van de EDEO;
- f) „gerubriceerde EU-informatie”: informatie of materiaal met een bepaalde EU-rubricering, waarvan ongeoorloofde openbaarmaking de belangen van de Europese Unie of van een of meer van haar lidstaten in meerdere of mindere mate kan schaden;

- g) „delegatie van de Unie”: delegaties in derde landen en internationale organisaties als bedoeld in artikel 1, lid 4, van Besluit 2010/427/EU van de Raad van 26 juli 2010 tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden.

Andere definities zijn opgenomen in de desbetreffende bijlagen en in aanhangsel A.

Artikel 3

Zorgplicht

1. De beveiligingsvoorschriften voor de EDEO hebben tot doel de zorgplicht van de EDEO te vervullen.
2. De zorgplicht van de EDEO omvat de inachtneming van de nodige zorgvuldigheid bij het treffen van alle redelijke maatregelen ter voorkoming van redelijkerwijs te voorziene schade voor de veiligheidsbelangen van de EDEO.

De zorgplicht omvat zowel beveiligings- als veiligheidsaspecten, onder meer die welke voortvloeien uit noodsituaties of crises van welke aard dan ook.

3. Met inachtneming van de zorgplicht van de lidstaten, de instellingen en organen van de EU en andere partijen met personeelsleden in de delegaties van de Unie en/of de locaties van delegaties van de Unie, en van de verantwoordelijkheid die de EDEO draagt wanneer delegaties van de Unie in genoemde werkruimten of in werkruimten van derden zijn ondergebracht, gaat de EDEO met elk van genoemde entiteiten administratieve regelingen aan waarin de respectieve rollen, taken en verantwoordelijkheden en mechanismen voor samenwerking zijn vastgelegd.

Artikel 4

Fysieke en infrastructurele beveiliging

1. De EDEO treft op alle locaties van de EDEO alle passende maatregelen (tijdelijk of permanent) op het gebied van fysieke beveiliging, waaronder regelingen voor toegangscontrole, ter bescherming van de veiligheidsbelangen van de EDEO. Bij het ontwerp en de planning van nieuwe locaties en voordat de EDEO bestaande locaties huurt, wordt met deze maatregelen rekening gehouden.
2. Aan onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden en personen te hunnen laste kunnen om veiligheidsredenen voor een specifieke periode en in specifieke zones bijzondere verplichtingen of beperkingen worden opgelegd.
3. De in de leden 1 en 2 bedoelde maatregelen moeten in passende verhouding staan tot het geschatte risico.

Artikel 5

Alarmtoestanden en beheer van crisissituaties

1. De veiligheidsautoriteit van de EDEO als bepaald in artikel 13, lid 1, afdeling 1, is verantwoordelijk voor het instellen van passende alarmtoestandsmaatregelen uit voorzorg of als reactie op gevaren en incidenten die de veiligheid binnen de EDEO in het gedrang brengen, en voor maatregelen voor het beheer van crisissituaties.
2. De in lid 1 bedoelde alarmtoestandsmaatregelen moeten in passende verhouding staan tot de mate van het gevaar voor de veiligheid. De alarmtoestandsniveaus worden vastgesteld in nauwe samenwerking met de bevoegde diensten van andere Europese instellingen, agentschappen en organen, en van de lidstaat of lidstaten die de EDEO huisvesten.
3. De veiligheidsautoriteit van de EDEO is het contactpunt in verband met de alarmtoestandsmaatregelen en het beheer van crisissituaties.

*Artikel 6***Bescherming van gerubriceerde informatie**

1. Voor de bescherming van gerubriceerde EU-informatie gelden de vereisten die bij dit besluit zijn vastgesteld, in het bijzonder in bijlage A. De houder van gerubriceerde EU-informatie is er verantwoordelijk voor dat de informatie aldus wordt beschermd.
2. De EDEO ziet erop toe dat slechts personen die aan de voorwaarden van bijlage A, artikel 5, voldoen, toegang krijgen tot gerubriceerde informatie.
3. De hoge vertegenwoordiger stelt tevens de voorwaarden vast waaronder plaatselijke functionarissen toegang krijgen tot gerubriceerde EU-informatie, overeenkomstig de in bijlage A bij dit besluit vastgestelde voorschriften voor de bescherming van gerubriceerde EU-informatie.
4. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, houdt een database bij van de veiligheidsmachtigingsstatus van alle onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden en contractanten van de EDEO.
5. Wanneer lidstaten gerubriceerde informatie met een nationale rubricering in de structuren of netwerken van de EDEO invoeren, beschermt de EDEO die informatie in overeenstemming met de voorschriften voor gerubriceerde EU-informatie op het gelijkwaardige beschermingsniveau dat volgens de toepasselijke voorschriften van aanhangsel B van dit besluit vereist is.
6. Zones binnen de EDEO waar informatie met de rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, of een daarmee gelijkwaardige rubricering, wordt opgeslagen, worden aangewezen als beveiligde zones overeenkomstig de krachtens bijlage A II bij dit besluit vastgestelde voorschriften en goedgekeurd door de veiligheidsautoriteit van de EDEO.
7. De procedures voor de uitvoering van de verantwoordelijkheden van de hoge vertegenwoordiger in het kader van overeenkomsten of administratieve regelingen betreffende de uitwisseling van gerubriceerde EU-informatie met derde landen of internationale organisaties worden beschreven in de bijlagen A en A VI bij dit besluit.
8. De secretaris-generaal bepaalt onder welke voorwaarden de EDEO de gerubriceerde EU-informatie die in zijn bezit is, kan delen met andere instellingen, organen of instanties van de Europese Unie. Daartoe wordt een adequaat kader opgezet, onder meer door interinstitutionele of andere daartoe vereiste regelingen te treffen.
9. Dit kader moet de garantie bieden dat gerubriceerde EU-informatie wordt beschermd in overeenstemming met de bijbehorende rubriceringsgraad en volgens basisbeginselen en minimumnormen die gelijkwaardig zijn aan die welke in dit besluit zijn neergelegd.

*Artikel 7***Veiligheidsincidenten en noodgevallen**

1. Om een tijdige en doeltreffende respons op veiligheidsincidenten te waarborgen, stelt de EDEO een proces in voor de melding van dergelijke incidenten en noodgevallen, dat vierentwintig uur per dag en zeven dagen per week operationeel is en berekend is op alle veiligheidsincidenten en bedreigingen voor de veiligheidsbelangen van de EDEO (bijvoorbeeld ongevallen, conflicten, kwaadwillige handelingen, criminele activiteiten, ontvoering en gijzeling, medische noodsituaties, incidenten met communicatie- en informatiesystemen, cyberaanvallen enz.).
2. Er worden noodverbindingskanalen tot stand gebracht tussen het hoofdkantoor van de EDEO, de delegaties van de Unie, de Raad, de Commissie, de speciale vertegenwoordigers van de EU en de lidstaten, teneinde deze te ondersteunen bij de beheersing van veiligheidsincidenten waarbij personeelsleden betrokken zijn, en de gevolgen daarvan, met inbegrip van noodplannen.
3. De beheersing van veiligheidsincidenten omvat onder meer:
 - procedures voor doeltreffende ondersteuning van het besluitvormingsproces in verband met veiligheidsincidenten waarbij personeel betrokken is, met inbegrip van besluiten betreffende de terugtrekking of schorsing van een missie, en
 - beleid en procedures voor het terughalen van personeelsleden die bijvoorbeeld vermist, ontvoerd of gegijzeld zijn, met inachtneming van de specifieke verantwoordelijkheden van de lidstaten, de EU-instellingen en de EDEO in dat verband. De behoefte aan specifieke vaardigheden in het kader van het beheer van dergelijke operaties wordt in aanmerking genomen, waarbij rekening wordt gehouden met de middelen die de lidstaten zouden kunnen verstrekken.

4. De EDEO stelt passende administratieve regelingen in voor het melden van veiligheids incidenten in delegaties van de Unie. Waar nodig worden de lidstaten, de Commissie, alle andere relevante autoriteiten en de desbetreffende beveiligingscomités ingelicht.
5. Het proces voor incidentenbeheersing wordt regelmatig geoefend en geëvalueerd.

Artikel 8

Beveiliging van communicatie- en informatiesystemen

1. De EDEO beschermt informatie die in communicatie- en informatiesystemen wordt verwerkt tegen bedreigingen voor de vertrouwelijkheid, integriteit, beschikbaarheid, authenticiteit en onweerlegbaarheid.
2. De veiligheidsautoriteit van de EDEO stelt voorschriften, een beveiligingsbeleid en een beveiligingsprogramma vast voor alle communicatie- en informatiesystemen die eigendom zijn van de EDEO of bij de EDEO in gebruik zijn.
3. De voorschriften, het beleid en het programma zijn in overeenstemming met die van de Raad en de Commissie en, waar nuttig, het beveiligingsbeleid van de lidstaten, en worden in nauwe coördinatie daarmee uitgevoerd.
4. Alle communicatie- en informatiesystemen worden aan een homologatieprocedure onderworpen. De EDEO past een systeem voor het beheer van veiligheidshomologatie toe in overleg met het secretariaat-generaal van de Raad en de Commissie.
5. Wanneer de gerubriceerde EU-informatie die de EDEO verwerkt, wordt beschermd met encryptieproducten, dienen die producten te zijn goedgekeurd door de autoriteit voor de goedkeuring van encryptieproducten van de EDEO, op aanbeveling van het Beveiligingscomité van de Raad.
6. De veiligheidsautoriteit van de EDEO stelt, voor zover nodig, de volgende information-assurancefuncties in:
 - a) een information-assuranceautoriteit;
 - b) een TEMPEST-autoriteit;
 - c) een autoriteit voor de goedkeuring van encryptieproducten;
 - d) een autoriteit voor de distributie van encryptieproducten.
7. Voor elk systeem stelt de veiligheidsautoriteit van de EDEO de volgende functies in:
 - a) een veiligheidshomologatieautoriteit;
 - b) een operationele autoriteit voor information assurance.
8. De bepalingen ter uitvoering van dit artikel wat de bescherming van gerubriceerde EU-informatie betreft, zijn in de bijlagen A en A IV opgenomen.

Artikel 9

Inbreuken op de beveiligingsvoorschriften en compromittering van gerubriceerde informatie

1. Een inbreuk op de beveiligingsvoorschriften is het resultaat van een handeling of nalatigheid in strijd met de beveiligingsvoorschriften van dit besluit en/of het beveiligingsbeleid of de beveiligingsrichtsnoeren die maatregelen voor de uitvoering van dit besluit omvatten, zoals goedgekeurd overeenkomstig artikel 21, lid 1.
2. Van compromittering van gerubriceerde informatie is sprake wanneer deze geheel of gedeeltelijk is bekendgemaakt aan onbevoegde personen of entiteiten.
3. Elke inbreuk of vermoedelijke inbreuk op de beveiligingsvoorschriften, alsook elke compromittering of vermoedelijke compromittering van gerubriceerde informatie, moet onmiddellijk worden gemeld aan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, dat passende maatregelen neemt overeenkomstig bijlage A, artikel 11.
4. Eenieder die verantwoordelijk is voor een inbreuk op de beveiligingsvoorschriften van dit besluit of voor de compromittering van gerubriceerde informatie, stelt zich bloot aan tuchtmaatregelen en/of rechtsvervolgning, overeenkomstig de geldende wet- en regelgeving, zoals bedoeld in bijlage A, artikel 11, lid 3.

*Artikel 10***Onderzoek van beveiligingsincidenten, inbreuken en/of compromittering, alsmede corrigerende maatregelen**

1. Onverminderd artikel 86 (tuchtmaatregelen) en bijlage IX bij het Statuut ⁽¹⁾ kan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, een veiligheidsonderzoek voeren:
 - a) bij mogelijk lekken, onjuiste afhandeling of roekeloze behandeling van gerubriceerde EU-informatie, gerubriceerde informatie van Euratom of gevoelige niet-gerubriceerde informatie;
 - b) als reactie op aanvallen van vijandige inlichtingendiensten tegen de EDEO en zijn personeelsleden;
 - c) als reactie op terroristische aanvallen tegen de EDEO en zijn personeelsleden;
 - d) bij cyberincidenten;
 - e) bij andere incidenten die gevolgen hebben of kunnen hebben voor de algemene veiligheid van de EDEO, met inbegrip van vermoede strafbare feiten.

2. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, neemt, waar nodig bijgestaan door deskundigen van de lidstaten en/of andere EU-instellingen, en waar nodig met toestemming van de veiligheidsautoriteit van de EDEO, wanneer en voor zover nodig de noodzakelijke corrigerende maatregelen die voortvloeien uit de onderzoeken.

Alleen personeelsleden die in het kader van hun huidige taken persoonlijk zijn gemandateerd door de veiligheidsautoriteit van de EDEO, kunnen de bevoegdheid krijgen de veiligheidsonderzoeken in de EDEO uit te voeren en te coördineren.

3. De onderzoekers moeten toegang hebben tot alle informatie die noodzakelijk is voor het uitvoeren van dergelijke onderzoeken en daarbij de volledige steun krijgen van alle diensten en personeelsleden van de EDEO.

De onderzoekers kunnen passende maatregelen nemen om bewijsmateriaal veilig te stellen, in overeenstemming met de ernst van de onderzochte situatie.

4. Wanneer de toegang tot informatie betrekking heeft op persoonsgegevens, waaronder persoonsgegevens in communicatie- en informatiesystemen, dient de toegang te voldoen aan Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad ⁽²⁾.

5. Wanneer het noodzakelijk is een onderzoeksdatabase op te zetten waarin persoonsgegevens zullen worden opgenomen, wordt de Europese Toezichthouder voor persoonsgegevens overeenkomstig genoemde verordening ingelicht.

*Artikel 11***Beheersing van beveiligingsrisico's**

1. Om te bepalen welke maatregelen moeten worden genomen om zijn veiligheid te beschermen, ontwikkelt de EDEO in nauwe samenwerking met het directoraat Beveiliging van de Europese Commissie en waar van toepassing de dienst Beveiliging van het secretariaat-generaal van de Raad een methode voor integrale beoordeling van de veiligheidsrisico's.

2. De risico's voor gerubriceerde EU-informatie worden beheerd als een proces. Dit proces wordt gericht op het bepalen van de bekende beveiligingsrisico's, het vaststellen van beveiligingsmaatregelen om deze risico's tot een aanvaardbaar niveau terug te dringen en het toepassen van deze maatregelen overeenkomstig het begrip „defence in depth”. De doeltreffendheid van deze maatregelen en het risiconiveau worden voortdurend geëvalueerd.

⁽¹⁾ Statuut van de ambtenaren van de Europese Unie en de Regeling welke van toepassing is op de andere personeelsleden, vastgesteld bij Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad (PB L 56 van 4.3.1968, blz. 1), hierna „het Statuut” genoemd,

⁽²⁾ Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

3. De bij dit besluit vastgestelde functies, verantwoordelijkheden en taken doen niets af aan de verantwoordelijkheid van elk onder de verantwoordelijkheid van de EDEO geplaatst personeelslid; met name EU-personeelsleden op dienstreis in derde landen dienen met gezond verstand en een goed oordeelsvermogen te werk te gaan wat hun eigen veiligheid betreft en alle toepasselijke veiligheidsvoorschriften, -regelingen, -procedures en -instructies na te leven.
4. Om veiligheidsrisico's te voorkomen en te controleren kan gemandateerd personeel antecedentenonderzoek verrichten naar personen die binnen de werkingssfeer van dit besluit vallen, om te bepalen of de verlening aan deze personen van toegang tot gebouwen van de EDEO of tot informatie een gevaar vormt voor de veiligheid. Daartoe hebben gemandateerde personeelsleden, overeenkomstig Verordening (EG) nr. 45/2001, toegang tot: a) alle informatiebronnen die ter beschikking staan van de EDEO, rekening houdend met de betrouwbaarheid van de informatiebron; b) de persoonlijke dossiers en de persoonsgegevens die de EDEO bijhoudt van zijn personeelsleden of toekomstige personeelsleden, of van contractanten in naar behoren gemotiveerde gevallen.
5. De EDEO neemt alle redelijke maatregelen om zijn veiligheidsbelangen te beschermen en redelijkerwijs te voorziene schade daaraan te voorkomen.
6. De in de EDEO geldende beveiligingsmaatregelen voor de bescherming van gerubriceerde EU-informatie gedurende de gehele levenscyclus daarvan moeten evenredig zijn met in het bijzonder de rubriceringsgraad, de vorm en de omvang van de informatie of het materiaal, de locatie en de constructie van de faciliteiten waar de gerubriceerde EU-informatie is ondergebracht en de dreiging, ook op lokaal niveau beoordeeld, van kwaadwillige en/of criminele activiteiten, met inbegrip van spionage, sabotage en terrorisme.

Artikel 12

Veiligheidsbesef en veiligheidsopleiding

1. De veiligheidsautoriteit van de EDEO ziet erop toe dat passende programma's voor veiligheidsbesef en veiligheidsopleiding worden opgezet en uitgevoerd, en dat de onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden en in voorkomend geval de personen te hunnen laste de nodige briefings inzake veiligheidsbesef en -opleiding krijgen, in overeenstemming met de risico's in de plaats waar zij werken of wonen.
2. Voordat toegang wordt verleend tot gerubriceerde EU-informatie, en vervolgens met regelmatige tussenpozen, worden alle personeelsleden geïnstrueerd over hun verantwoordelijkheden, en erkennen zij deze, met betrekking tot de bescherming van gerubriceerde EU-informatie overeenkomstig de krachtens artikel 6 vastgestelde voorschriften.

Artikel 13

Organisatie van de beveiliging binnen de EDEO

Afdeling 1

Algemene bepalingen

1. De secretaris-generaal is de veiligheidsautoriteit van de EDEO. In die hoedanigheid ziet de secretaris-generaal erop toe dat:
 - a) de beveiligingsmaatregelen waar nodig worden gecoördineerd met de bevoegde autoriteiten van de lidstaten, het secretariaat-generaal van de Raad en de Commissie en in voorkomend geval derde landen of internationale organisaties, met betrekking tot alle beveiligingsaangelegenheden die voor de activiteiten van de EDEO relevant zijn, ook wat betreft de aard van risico's voor de veiligheidsbelangen van de EDEO en de middelen om zich tegen die risico's te beschermen;
 - b) de beveiligingsaspecten bij alle activiteiten van de EDEO vanaf het eerste begin in aanmerking worden genomen;
 - c) slechts personen die aan de voorwaarden van bijlage A, artikel 5, voldoen, toegang krijgen tot gerubriceerde informatie;
 - d) een registratiesysteem wordt opgezet dat waarborgt dat informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt verwerkt overeenkomstig dit besluit, zowel binnen de EDEO als na vrijgave aan lidstaten van de EU, instellingen, organen of instanties van de EU en andere toegelaten ontvangers. Er wordt een afzonderlijk register bijgehouden van alle gerubriceerde EU-informatie die door de EDEO wordt vrijgegeven aan derde staten of internationale organisaties, en van alle gerubriceerde informatie die van derde staten of internationale organisaties wordt ontvangen;
 - e) de in artikel 16 bedoelde veiligheidsinspecties worden verricht;

- f) onderzoek wordt gedaan naar alle inbreuken of vermoedelijke inbreuken op de beveiligingsvoorschriften, alsmede compromittering of verlies of vermoedelijke compromittering of verlies van gerubriceerde informatie die in het bezit of afkomstig van de EDEO is, en dat de bevoegde veiligheidsautoriteiten om hulp wordt verzocht bij die onderzoeken;
- g) passende plannen en mechanismen voor incidenten- en gevolgenbeheersing worden opgezet om bij veiligheidsincidenten tijdig en doeltreffend te kunnen optreden;
- h) passende maatregelen worden getroffen wanneer personen dit besluit niet naleven;
- i) passende fysieke en organisatorische maatregelen zijn ingesteld voor de bescherming van de veiligheidsbelangen van de EDEO.

De veiligheidsautoriteit van de EDEO:

- stelt in overleg met de Commissie de veiligheidscategorie van de delegaties van de Unie vast;
- beslist, waar nodig, na overleg met de hoge vertegenwoordiger, wanneer personeelsleden van een delegatie van de Unie in verband met de veiligheidssituatie moeten worden geëvacueerd;
- beslist welke maatregelen in voorkomend geval moeten worden genomen voor de bescherming van personen ten laste van onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden, rekening houdende met regelingen die met de EU-instellingen zijn overeengekomen, zoals bedoeld in artikel 3, lid 3;
- keurt het beleid voor versleutelde communicatie goed, in het bijzonder het programma voor de installatie van encryptieproducten en het encryptiemechanisme.

2. De veiligheidsautoriteit van de EDEO wordt bij deze taak bijgestaan door de directeur-generaal begroting en administratie, de EDEO-directeur die verantwoordelijk is voor beveiliging en, waar nodig, de adjunct-secretaris-generaal EVDB en crisisrespons.

3. De secretaris-generaal kan als veiligheidsautoriteit van de EDEO indien nodig de daarbij behorende taken delegeren.

4. De hoofden van afdelingen/divisies zijn verantwoordelijk voor de tenuitvoerlegging van de voorschriften inzake de bescherming van gerubriceerde EU-informatie in hun afdeling/divisie.

Met behoud van de genoemde verantwoordelijkheid wijst elk hoofd van een afdeling/divisie een personeelslid aan voor de functie van afdelingsveiligheidscoördinator, met dien verstande dat deze kan beschikken over middelen die evenredig zijn met de door die afdeling/divisie verwerkte gerubriceerde EU-informatie.

De afdelingsveiligheidscoördinatoren staan, wanneer en voor zover nodig, het hoofd van hun afdeling/divisie bij en bieden hem ondersteuning bij de uitvoering van veiligheidsgerelateerde taken, zoals:

- a) het ontwikkelen van aanvullende veiligheidseisen voor de specifieke behoeften van de afdeling/divisie;
- b) het houden van periodieke veiligheidsbriefings voor de leden van de afdeling/divisie;
- c) het toezien op de naleving van het beginsel van „noodzaak tot kennisname” in hun afdeling/divisie;
- d) het up-to-date houden van de lijst van safecodes en -sleutels;
- e) het handhaven van de veiligheidsprocedures en -maatregelen;
- f) het melden van inbreuken op de veiligheidsvoorschriften of compromittering van gerubriceerde EU-informatie aan de directeur en het directoraat dat verantwoordelijk is voor beveiliging;
- g) het debriefen van personeelsleden die hun dienstverband bij de EDEO beëindigen;
- h) regelmatige rapportage, langs hiërarchische weg, over veiligheidsaangelegenheden van de afdeling/divisie;
- i) het contact over veiligheidsaangelegenheden met het directoraat van de EDEO dat verantwoordelijk is voor beveiliging.

Elke activiteit of aangelegenheid die veiligheidsconsequenties kan hebben, moet tijdig worden gemeld aan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging gemeld.

5. De hoofden van de delegaties zijn verantwoordelijk voor de tenuitvoerlegging van alle maatregelen betreffende de beveiliging van de delegatie.

Afdeling 2

Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging

1. De EDEO heeft een directoraat dat verantwoordelijk is voor beveiliging en dat:
 - a) alle beveiligingsmaatregelen op alle locaties die onder de verantwoordelijkheid van de EDEO vallen, zowel op het hoofdkantoor als elders in de EU en in derde landen, beheert, coördineert, superviseert en/of uitvoert;
 - b) erop toeziet dat alle activiteiten die consequenties kunnen hebben voor de bescherming van de veiligheidsbelangen van de EDEO in overeenstemming zijn met dit besluit en de uitvoeringsbepalingen daarvan;
 - c) optreedt als hoofdadviseur van de hoge vertegenwoordiger, de veiligheidsautoriteit van de EDEO en de adjunct-secretaris-generaal over alle aangelegenheden die met de beveiliging samenhangen;
 - d) wordt bijgestaan door de bevoegde diensten van de lidstaten, overeenkomstig artikel 10, lid 3, van Besluit 2010/427/EU van de Raad tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden;
 - e) de activiteiten van de veiligheidshomologatieautoriteit van de EDEO ondersteunt door de fysieke veiligheid te beoordelen van de algemene beveiligingsomgeving (General Security Environment — GSE)/lokale beveiligingsomgeving (Local Security Environment — LSE) van de communicatie- en informatiesystemen die gerubriceerde EU-informatie verwerken en van de locaties waarvoor een machtiging tot verwerking en opslag van gerubriceerde EU-informatie wordt verleend.
2. De directeur van de EDEO die verantwoordelijk is voor beveiliging, is verantwoordelijk voor:
 - a) de algemene bescherming van de veiligheidsbelangen van de EDEO;
 - b) het opstellen, herzien en actualiseren van de beveiligingsvoorschriften en het coördineren van de veiligheidsmaatregelen met de bevoegde autoriteiten van de lidstaten en, waar van toepassing, de bevoegde autoriteiten van derde staten en internationale organisaties waarmee de EU beveiligingsovereenkomsten en/of -regelingen heeft gesloten;
 - c) de ondersteuning van de werkzaamheden van het Beveiligingscomité van de EDEO, zoals bedoeld in artikel 15, lid 1, van dit besluit;
 - d) de eventuele contacten op het gebied van beveiligingsaangelegenheden met andere partners en autoriteiten dan de onder b) bedoelde;
 - e) de prioritering en het doen van voorstellen voor het beheer van de beveiligingsbegroting op het hoofdkantoor en in de delegaties van de Unie.
3. Het hoofd van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging:
 - a) ziet erop toe dat inbreuken op de beveiligingsvoorschriften en compromittering worden geregistreerd en dat er, waar en wanneer nodig, onderzoek naar wordt gedaan;
 - b) komt regelmatig, alsook telkens wanneer dat noodzakelijk is, bijeen met de directeur Beveiliging van het secretariaat-generaal van de Raad en de directeur van het directoraat Beveiliging van de Commissie om aangelegenheden van gemeenschappelijk belang te bespreken.
4. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, bouwt contact en nauwe samenwerking op met:
 - de met de beveiliging belaste diensten van de ministeries van Buitenlandse Zaken van de lidstaten;
 - de nationale veiligheidsautoriteiten en/of andere bevoegde veiligheidsautoriteiten van de lidstaten, teneinde hun medewerking te verkrijgen voor informatie die noodzakelijk is voor het beoordelen van gevaren en bedreigingen waaraan de EDEO, zijn personeel, zijn activiteiten en middelen en zijn gerubriceerde informatie blootstaan op de gebruikelijke plaats waar de EDEO zijn werkzaamheden uitvoert;
 - de bevoegde veiligheidsautoriteiten van de lidstaten of ontvangende staten op het grondgebied waarvan de EDEO activiteiten kan uitoefenen, betreffende aangelegenheden die verband houden met de bescherming van zijn personeel, zijn activiteiten, zijn activa en middelen en zijn gerubriceerde informatie op dat grondgebied;
 - de dienst Beveiliging van het secretariaat-generaal van de Raad en het directoraat Beveiliging van het directoraat-generaal Personele Middelen en Veiligheid van de Europese Commissie, alsmede in voorkomend geval de beveiligingsdiensten van andere instellingen, organen en instanties van de EU;
 - de beveiligingsdiensten van derde staten of internationale organisaties, met het oog op nuttige coördinatie, en
 - de nationale veiligheidsautoriteiten van de lidstaten, met betrekking tot alle vraagstukken die verband houden met de bescherming van gerubriceerde EU-informatie.

Afdeling 3

Delegaties van de Unie

1. De hoofden van de delegaties zijn verantwoordelijk voor de tenuitvoerlegging en het beheer ter plaatse van alle maatregelen die verband houden met de bescherming van de veiligheidsbelangen van de EDEO binnen de locaties van de delegatie die onder de bevoegdheid van de delegatie vallen.

In overleg met de bevoegde autoriteiten van de ontvangende staat, waar nodig, nemen zij alle redelijkerwijs uitvoerbare maatregelen om ervoor te zorgen dat daartoe passende fysieke en organisatorische maatregelen zijn getroffen.

Het hoofd van de delegatie stelt waar nodig beveiligingsprocedures vast voor de bescherming van personen ten laste als bedoeld in artikel 2, onder c), rekening houdende met administratieve regelingen zoals bedoeld in artikel 3, lid 3. Het hoofd van de delegatie brengt verslag uit over alle beveiligingsgerelateerde vraagstukken die onder zijn bevoegdheid vallen aan het hoofd van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging.

Het hoofd wordt bij deze taken bijgestaan door het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, door het beveiligingsbeheersteam van de delegatie dat bestaat uit personeel dat specifieke taken en functies op beveiligingsgebied uitvoert en indien nodig door speciaal beveiligingspersoneel.

De delegatie bouwt contact en nauwe samenwerking op met diplomatieke missies van de lidstaten op het gebied van beveiligingsaangelegenheden.

2. Bovendien zal het hoofd van de delegatie:

- uitvoerige beveiligings- en rampenplannen voor de delegatie vaststellen op basis van generieke operationele standaardprocedures;
- vierentwintig uur per dag, zeven dagen per week, een doeltreffend systeem voor het beheer van veiligheidsincidenten en noodsituaties binnen de actieradius van de delegatie operationeel houden;
- erop toezien dat al het in de delegatie ingezette personeel gedekt is door een op de omstandigheden in het gebied afgestemde verzekering;
- erop toezien dat beveiliging onderdeel is van de introductieopleiding van de delegatie, die al het in de delegatie ingezette personeel voor of bij de aankomst in de delegatie ontvangt, en
- erop toezien dat naar aanleiding van beveiligingsbeoordelingen geformuleerde aanbevelingen worden opgevolgd en op gezette tijden over de uitvoering ervan en over andere veiligheidskwesties schriftelijk verslag uitbrengen aan de veiligheidsautoriteit van de EDEO.

3. Het hoofd van de delegatie blijft verantwoordelijk en aansprakelijk voor de instandhouding van het beveiligingsbeheer en het behoud van de veerkracht van de organisatie, maar kan de uitvoering van zijn of haar beveiligingstaken delegeren aan de veiligheidscoördinator van de delegatie; die functie wordt uitgeoefend door het adjunct-hoofd van delegatie ofwel, indien niemand in die functie is benoemd, een passende andere functionaris.

De veiligheidscoördinator van de delegatie kan in het bijzonder met de volgende taken worden belast:

- het coördineren van de veiligheidsfuncties in de delegatie;
- het onderhouden van contact over beveiligingsaangelegenheden met de bevoegde autoriteiten van de ontvangende staat en met collega's in de ambassades en diplomatieke missies van de lidstaten;
- het uitvoeren van passende procedures voor beveiligingsbeheer met betrekking tot de veiligheidsbelangen van de EDEO, waaronder de bescherming van gerubriceerde EU-informatie;
- het waarborgen van het naleven van de beveiligingsvoorschriften en -instructies;
- het instrueren van de personeelsleden over de voor hen geldende beveiligingsvoorschriften en de specifieke risico's in de ontvangende staat;
- het indienen van verzoeken aan het directoraat van de EDEO dat verantwoordelijk is voor veiligheidsmachtigingen, met betrekking tot posten waarvoor een veiligheidsmachtiging voor personen vereist is, en
- het op de hoogte houden van het hoofd van de delegatie, de regionale beveiligingsfunctionaris (hierna „RSO” genoemd) en het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, over incidenten en ontwikkelingen op het terrein die van invloed zijn op de bescherming van de veiligheidsbelangen van de EDEO.

4. Het hoofd van de delegatie kan beveiligingstaken van administratieve of technische aard delegeren aan het hoofd van de administratie en andere personeelsleden van de delegatie van de Unie.

5. De delegatie van de Unie wordt bijgestaan door een RSO. De RSO's vervullen in de delegaties de onderstaande taken binnen de geografische gebieden waarvoor zij verantwoordelijk zijn.

In bepaalde omstandigheden, wanneer de veiligheidssituatie daartoe noopt, kan een speciale RSO op een voltijds residentiële post aan een specifieke delegatie worden toegewezen.

RSO's kunnen verplicht worden te verhuizen naar een gebied buiten hun normale werkterrein, met inbegrip van het hoofdkantoor, of in welk land dan ook een residentiële post aan te nemen overeenkomstig de veiligheidssituatie of wanneer dat noodzakelijk is volgens het directoraat van de EDEO dat verantwoordelijk is voor beveiliging.

6. De RSO's staan rechtstreeks onder het operationeel gezag van de EDEO-dienst van het hoofdkantoor die verantwoordelijk is voor het veiligheidsbeleid ter plaatse, maar onder het gezamenlijke administratieve gezag van die dienst en het hoofd van de delegatie waar zij werken. Zij verlenen het hoofd en het personeel van de delegatie advies en bijstand bij het opzetten en uitvoeren van alle fysieke, organisatorische en procedurele maatregelen in verband met de veiligheid van de delegatie.

7. De RSO's verlenen het hoofd en het personeel van de delegatie advies en steun. Waar nuttig, met name wanneer een RSO een voltijds residentiële post bekleedt, kan deze een delegatie van de Unie bijstand verlenen bij het beheer en de uitvoering van de beveiliging, onder meer wat het opstellen van beveiligingscontracten en het beheer van homologaties en veiligheidsmachtigingen betreft.

Artikel 14

Operaties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) en de speciale vertegenwoordigers van de EU

Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, verleent bijstand en advies aan de directeur van het directoraat Crisisbeheersing en Planning, de directeur-generaal van de Militaire Staf van de EU, de civiele operationele commandant die de Civiele Plannings- en Uitvoeringcapaciteit leidt, en de militaire operationele commandanten van de EU met betrekking tot de beveiligingsaspecten van de GVDB-operaties, en aan de speciale vertegenwoordigers van de EU met betrekking tot de beveiligingsaspecten van hun mandaat, ter aanvulling op de specifieke bepalingen op dit gebied die deel uitmaken van het desbetreffende beleid dat door de Raad is vastgesteld.

Artikel 15

Beveiligingscomité van de EDEO

1. Er wordt een Beveiligingscomité van de EDEO ingesteld.

Het Beveiligingscomité wordt voorgezeten door de veiligheidsautoriteit van de EDEO of een door deze aangewezen vertegenwoordiger, en komt bijeen op instructie van de voorzitter of op verzoek van een lid. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, steunt de voorzitter bij deze taak en verleent waar nodig administratieve bijstand ten behoeve van de werkzaamheden van het comité.

2. Het Beveiligingscomité van de EDEO bestaat uit vertegenwoordigers van:

- elke lidstaat;
- de dienst Beveiliging van het secretariaat-generaal van de Raad;
- het directoraat Beveiliging van het directoraat-generaal Personele Middelen en Veiligheid van de Europese Commissie.

Een delegatie van een lidstaat bij het Beveiligingscomité van de EDEO kan bestaan uit leden van:

- de nationale veiligheidsautoriteit en/of de aangewezen veiligheidsautoriteit;
- de met de beveiliging belaste diensten van het Ministerie van Buitenlandse Zaken.

3. De vertegenwoordigers in het comité kunnen zich, als zij dat nodig achten, laten vergezellen en adviseren door deskundigen. Vertegenwoordigers van andere EU-instellingen, -organen of -instanties kunnen worden uitgenodigd vergaderingen bij te wonen wanneer voor hun beveiliging relevante vraagstukken worden besproken.

4. Onverminderd lid 5 verleent het Beveiligingscomité van de EDEO bijstand aan de EDEO betreffende alle beveiligingsvraagstukken die voor de activiteiten van de EDEO relevant zijn, in de vorm van advies aan het hoofdkantoor en de delegaties van de Unie.

Onverminderd lid 5:

a) wordt het Beveiligingscomité van de EDEO met name geraadpleegd over:

- beveiligingsbeleid en -richtsnoeren, concepten en andere methodologische documentatie met betrekking tot beveiliging, in het bijzonder ten aanzien van de bescherming van gerubriceerde informatie en de maatregelen die moeten worden genomen wanneer een EDEO-personeelslid de beveiligingsvoorschriften niet naleeft;
- technische beveiligingsaspecten die van invloed kunnen zijn op de beslissing van de hoge vertegenwoordiger om de Raad aan te bevelen onderhandelingen te openen over beveiligings- of informatieovereenkomsten als bedoeld in bijlage A, artikel 10, lid 1, onder a);
- elke wijziging van dit besluit;

b) kan het Beveiligingscomité van de EDEO, naargelang van het geval, worden geraadpleegd of ingelicht over vraagstukken betreffende de beveiliging van het personeel en de activa in het hoofdkantoor van de EDEO en de delegaties van de Unie, zulks onverminderd artikel 3, lid 3;

c) wordt het Beveiligingscomité ingelicht over elk binnen de EDEO geconstateerd geval van compromittering of verlies van gerubriceerde EU-informatie.

5. Voor elke wijziging van de in dit besluit en in bijlage A daarbij opgenomen voorschriften inzake de bescherming van gerubriceerde EU-informatie is een unaniem gunstig advies van de in het Beveiligingscomité van de EDEO vertegenwoordigde lidstaten vereist. Een unaniem gunstig advies is tevens vereist voordat:

- onderhandelingen worden geopend over administratieve regelingen als bedoeld in bijlage A, artikel 10, lid 1, onder b);
- gerubriceerde informatie wordt vrijgegeven in de uitzonderlijke omstandigheden bedoeld in bijlage A VI, punten 9, 11 en 12;
- de verantwoordelijkheid van de opsteller van de informatie wordt overgenomen in de omstandigheden bedoeld in bijlage A, artikel 10, lid 6, laatste zin.

Wanneer een unaniem gunstig advies is vereist, wordt aan die voorwaarde voldaan wanneer geen van de delegaties van de lidstaten tijdens de werkzaamheden van het comité bezwaren uit.

6. Het Beveiligingscomité van de EDEO houdt ten volle rekening met het beveiligingsbeleid en de beveiligingsrichtsnoeren die bij de Raad en de Commissie van kracht zijn.

7. Het Beveiligingscomité van de EDEO ontvangt de lijst van jaarlijkse EDEO-inspecties en de inspectierapporten, zodra deze zijn opgesteld.

8. Organisatie van vergaderingen:

- het Beveiligingscomité van de EDEO komt ten minste twee keer per jaar bijeen. Extra bijeenkomsten, zowel in de volledige samenstelling als in de formatie „nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten” of de formatie „ministeries van Buitenlandse Zaken”, kunnen door de voorzitter of op verzoek van de leden van het comité worden bijeengeroepen;
- het Beveiligingscomité van de EDEO organiseert zijn werkzaamheden zodanig dat het aanbevelingen over specifieke beveiligingsgebieden kan verstrekken. Het kan zo nodig andere deelgebieden van deskundigheid vaststellen. Het stelt mandaten voor deze deelgebieden van deskundigheid vast en ontvangt verslagen over de desbetreffende activiteiten;
- het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, is belast met de voorbereiding van de te bespreken agendapunten. De voorzitter stelt voor elke vergadering de voorlopige agenda op. De leden van het comité kunnen andere te bespreken punten voorstellen.

*Artikel 16***Veiligheidsinspecties**

1. De veiligheidsautoriteit van de EDEO ziet erop toe dat regelmatig veiligheidsinspecties worden verricht op het hoofdkantoor van de EDEO en in de delegaties van de Unie, teneinde te beoordelen of de beveiligingsmaatregelen toereikend en in overeenstemming met dit besluit zijn. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, kan waar nodig deskundigen aanwijzen om deel te nemen aan veiligheidsinspecties van EU-organen en -instanties die uit hoofde van titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie zijn opgericht.

2. De veiligheidsinspecties van de EDEO worden uitgevoerd onder het gezag van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, en, waar nodig, met steun van beveiligingsexperts die andere EU-instellingen of lidstaten vertegenwoordigen, met name in het kader van de in artikel 3, lid 3, bedoelde regelingen.

3. De EDEO kan waar nodig gebruikmaken van deskundigheid in de lidstaten, het secretariaat-generaal van de Raad en de Europese Commissie.

Waar nodig kunnen beveiligingsexperts die werkzaam zijn in missies van lidstaten in derde landen en/of vertegenwoordigers van de diplomatieke beveiligingsdiensten van de lidstaten worden uitgenodigd om aan de veiligheidsinspectie van een delegatie van de Unie deel te nemen.

4. De bepalingen ter uitvoering van dit artikel, wat de bescherming van gerubriceerde EU-informatie betreft, zijn in bijlage A III opgenomen.

*Artikel 17***Evaluatiebezoeken**

Er worden evaluatiebezoeken geregeld om de doeltreffendheid te verifiëren van de door een derde staat of een internationale organisatie genomen maatregelen ter bescherming van gerubriceerde EU-informatie die wordt uitgewisseld in het kader van een administratieve regeling als bedoeld in bijlage A, artikel 10, lid 1, onder b).

Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, kan deskundigen aanwijzen om deel te nemen aan evaluatiebezoeken aan derde staten of internationale organisaties waarmee de EU een informatiebeveiligingsovereenkomst als bedoeld in bijlage A, artikel 10, lid 1, onder a), heeft gesloten.

*Artikel 18***Bedrijfscontinuïteitsplan**

Bij het beheer van de veiligheidsgerelateerde aspecten van de bedrijfsprocessen van de EDEO in het kader van het algemene bedrijfscontinuïteitsplan van de EDEO wordt de veiligheidsautoriteit van de EDEO bijgestaan door het directoraat van de EDEO dat verantwoordelijk is voor beveiliging.

*Artikel 19***Reisadvies voor dienstreizen buiten de EU**

Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, ziet erop toe dat reisadvies wordt verleend ten behoeve van dienstreizen buiten de EU van onder de verantwoordelijkheid van de EDEO geplaatst personeel, waarbij een beroep wordt gedaan op de middelen van alle relevante diensten van de EDEO — in het bijzonder de SITROOM, het INTSEN, de geografische afdelingen en de delegaties van de Unie.

Op verzoek verstrekt het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, met gebruikmaking van bovengenoemde bronnen, specifiek reisadvies ten behoeve van dienstreizen van onder de verantwoordelijkheid van de EDEO geplaatst personeel naar derde landen met een hoog risico of een verhoogd risiconiveau.

*Artikel 20***Gezondheid en veiligheid**

De beveiligingsvoorschriften van de EDEO vormen een aanvulling op de voorschriften van de EDEO voor de bescherming van de gezondheid en veiligheid, die door de hoge vertegenwoordiger zijn vastgesteld.

*Artikel 21***Uitvoering en toetsing**

1. De veiligheidsautoriteit van de EDEO stelt, waar nodig na overleg met het Beveiligingscomité van de EDEO, beveiligingsrichtsnoeren op tot vaststelling van alle maatregelen die noodzakelijk zijn voor de tenuitvoerlegging van deze voorschriften binnen de EDEO, en brengt in nauwe samenwerking met de bevoegde veiligheidsautoriteiten van de lidstaten en met de steun van de relevante diensten van de EU-instellingen de noodzakelijke capaciteit inzake alle aspecten van beveiliging tot stand.
2. Overeenkomstig artikel 4, lid 5, van Besluit 2010/427/EU van de Raad van 26 juli 2010 tot vaststelling van de organisatie en werking van de Europese Dienst voor extern optreden kan zo nodig gebruik worden gemaakt van overgangsregelingen in de vorm van overeenkomsten inzake het dienstverleningsniveau met de relevante diensten van het secretariaat-generaal van de Raad en de Commissie.
3. De hoge vertegenwoordiger ziet toe op de algehele samenhang bij de toepassing van dit besluit en draagt zorg voor voortdurende toetsing van deze beveiligingsvoorschriften.
4. De beveiligingsvoorschriften van de EDEO worden ten uitvoer gelegd in nauwe samenwerking met de bevoegde veiligheidsautoriteiten van de lidstaten.
5. De EDEO ziet erop toe dat het crisisresponsstelsel van de EDEO met alle aspecten van het beveiligingsproces rekening houdt.
6. De secretaris-generaal, in zijn hoedanigheid van veiligheidsautoriteit, en het hoofd van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, zien toe op de tenuitvoerlegging van dit besluit.

*Artikel 22***Vervanging van voorgaande besluiten**

Het besluit van de hoge vertegenwoordiger van de Unie voor Buitenlandse Zaken en Veiligheidsbeleid van 19 april 2013 betreffende de beveiligingsvoorschriften voor de Europese Dienst voor extern optreden wordt bij onderhavig besluit ingetrokken en erdoor vervangen ⁽¹⁾.

*Artikel 23***Slotbepalingen**

Dit besluit treedt in werking op de datum waarop het wordt ondertekend.

Het wordt bekendgemaakt in het Publicatieblad van de Europese Unie.

De bevoegde autoriteiten van de EDEO stellen alle personeelsleden op wie dit besluit en de bijlagen erbij van toepassing zijn, tijdig in kennis van de inhoud en de inwerkingtreding van dit besluit en van alle later wijzigingen ervan.

Gedaan te Brussel, 19 september 2017.

Federica MOGHERINI

*Hoge vertegenwoordiger van de Unie voor buitenlandse zaken
en veiligheidsbeleid*

⁽¹⁾ PB C 190 van 29.6.2013, blz. 1.

BIJLAGE A

BEGINSELEN EN NORMEN VOOR DE BESCHERMING VAN GERUBRICEERDE EU-INFORMATIE*Artikel 1***Doel, toepassingsgebied en definities**

1. In deze bijlage worden de grondbeginselen en minimumnormen voor beveiliging vastgesteld ten behoeve van de bescherming van gerubriceerde EU-informatie.
2. Deze grondbeginselen en minimumnormen zijn van toepassing op de EDEO en op onder de verantwoordelijkheid van de EDEO geplaatst personeel, zoals bedoeld in artikel 1 en gedefinieerd in artikel 2 van dit besluit.

*Artikel 2***Definitie van gerubriceerde EU-informatie, rubriceringen en markeringen**

1. Gerubriceerde EU-informatie is informatie of materiaal met een bepaalde EU-rubricering, waarvan ongeoorloofde openbaarmaking de belangen van de Europese Unie of van een of meer van haar lidstaten in meerdere of mindere mate kan schaden.
2. Voor gerubriceerde EU-informatie worden de volgende rubriceringen gehanteerd:
 - a) TRÈS SECRET UE/EU TOP SECRET: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten uitzonderlijk ernstig kan schaden;
 - b) SECRET UE/EU SECRET: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten ernstig kan schaden;
 - c) CONFIDENTIEL UE/EU CONFIDENTIAL: informatie en materiaal waarvan de ongeoorloofde openbaarmaking de wezenlijke belangen van de Europese Unie of van een of meer van haar lidstaten kan schaden;
 - d) RESTREINT UE/EU RESTRICTED: informatie en materiaal waarvan de ongeoorloofde openbaarmaking nadelig kan zijn voor de belangen van de Europese Unie of van een of meer van haar lidstaten.
3. Gerubriceerde EU-informatie krijgt een rubricering overeenkomstig lid 2. Daarnaast kunnen er markeringen op worden aangebracht om de gebieden waarop zij betrekking heeft aan te duiden, de opsteller te identificeren, de verspreiding of het gebruik te beperken of de geschiktheid voor vrijgave aan te geven.

*Artikel 3***Rubriceringsbeheer**

1. De EDEO zorgt ervoor dat gerubriceerde EU-informatie naar behoren wordt gerubriceerd en duidelijk als gerubriceerde informatie wordt aangemerkt, en dat de rubriceringsgraad ervan slechts zolang als nodig wordt behouden.
2. Gerubriceerde EU-informatie wordt niet lager gerubriceerd of gederubriceerd en de in artikel 2, lid 3, bedoelde markeringen worden niet gewijzigd of verwijderd zonder voorafgaande schriftelijke toestemming van de opsteller.
3. De veiligheidsautoriteit van de EDEO stelt, na raadpleging van het Beveiligingscomité van de EDEO overeenkomstig artikel 15, lid 5, van dit besluit, beveiligingsrichtsnoeren inzake het genereren van gerubriceerde EU-informatie vast, met inbegrip van een praktische rubriceringsgids.

*Artikel 4***Bescherming van gerubriceerde informatie**

1. Gerubriceerde EU-informatie wordt beschermd in overeenstemming met dit besluit.
2. De houder van alle gerubriceerde EU-informatie is verantwoordelijk voor de bescherming ervan in overeenstemming met dit besluit.

3. Wanneer lidstaten gerubriceerde informatie met een nationale rubricering in de structuren of netwerken van de EDEO invoeren, beschermt de EDEO die informatie in overeenstemming met de voorschriften voor gerubriceerde EU-informatie op het gelijkwaardige beschermingsniveau dat volgens de toepasselijke voorschriften van aanhangsel B vereist is.

De EDEO stelt passende procedures vast voor de nauwkeurige registratie van de opsteller van:

- gerubriceerde informatie die de EDEO heeft ontvangen, en
- bronnenmateriaal dat vervat is in gerubriceerde informatie die door de EDEO is opgesteld.

Het Beveiligingscomité van de EDEO wordt van deze procedures in kennis gesteld.

4. Het is mogelijk dat grote hoeveelheden of een compilatie van gerubriceerde EU-informatie een beschermingsniveau vereisen dat overeenstemt met een hogere rubriceringsgraad dan die van de onderdelen ervan.

Artikel 5

Persoonsgerelateerde beveiliging voor de verwerking van gerubriceerde EU-informatie

1. Personeelsgerelateerde beveiliging is de toepassing van maatregelen die ervoor moeten zorgen dat toegang tot gerubriceerde EU-informatie uitsluitend wordt verleend aan personen die:

- een „noodzaak tot kennisname” hebben,
- wat de toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger betreft, een veiligheidsmachtiging voor het passende niveau hebben of anderszins uit hoofde van hun functie daartoe naar behoren zijn gemachtigd in overeenstemming met de nationale wet- en regelgeving, en
- zijn geïnstrueerd over hun verantwoordelijkheden.

2. In de procedures inzake veiligheidsmachtigingen voor personen wordt bepaald of een persoon, gelet op diens loyaliteit en betrouwbaarheid, toegang kan worden verleend tot gerubriceerde EU-informatie.

3. Voordat hun toegang tot gerubriceerde EU-informatie wordt verleend, en vervolgens met regelmatige tussenpozen, worden alle personen geïnstrueerd over hun verantwoordelijkheden ter bescherming van gerubriceerde EU-informatie overeenkomstig dit besluit, en dienen zij deze verantwoordelijkheden schriftelijk te bevestigen.

4. De bepalingen ter uitvoering van dit artikel zijn in bijlage A I opgenomen.

Artikel 6

Fysieke beveiliging van gerubriceerde EU-informatie

1. Fysieke beveiliging is de toepassing van fysieke en technische beschermingsmaatregelen om toegang zonder machtiging tot gerubriceerde EU-informatie te ontmoedigen.

2. Met de fysieke beveiligingsmaatregelen wordt beoogd het binnendringen met list of geweld te verhinderen, acties waarvoor geen toestemming is verleend af te schrikken, tegen te gaan en op te sporen en op basis van het „noodzaak tot kennisname”-beginsel een onderscheid tussen personeelsleden mogelijk te maken wat betreft de toegang tot gerubriceerde EU-informatie. Deze maatregelen worden op een risicobeheersingsproces gebaseerd.

3. Er worden fysieke beveiligingsmaatregelen ingesteld voor alle locaties, gebouwen, kantoren, ruimten en andere zones waar gerubriceerde EU-informatie wordt verwerkt of opgeslagen, met inbegrip van zones waar communicatie- en informatiesystemen, zoals gedefinieerd in bijlage A, artikel 8, lid 2, zijn ondergebracht.

4. Zones waar gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt opgeslagen, worden overeenkomstig bijlage A II als beveiligde zones aangemerkt en door de veiligheidsautoriteit van de EDEO goedgekeurd.

5. Voor de bescherming van gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger worden uitsluitend goedgekeurde apparatuur en voorzieningen gebruikt.

6. De bepalingen ter uitvoering van dit artikel zijn in bijlage A II opgenomen.

Artikel 7

Beheer van gerubriceerde informatie

1. Het beheer van gerubriceerde informatie is het toepassen van administratieve maatregelen voor het controleren van gerubriceerde EU-informatie gedurende de gehele levenscyclus ervan, teneinde de in de artikelen 5, 8 en 6 bedoelde maatregelen aan te vullen, en daarbij het al dan niet opzettelijk compromitteren of verliezen van die informatie te helpen voorkomen, opsporen en herstellen. Die maatregelen hebben met name betrekking op het genereren, registreren, kopiëren, vertalen, vervoeren, verwerken, opslaan en vernietigen van gerubriceerde EU-informatie.
2. Informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt vóór verspreiding en bij ontvangst geregistreerd voor beveiligingsdoeleinden. De bevoegde autoriteiten in de EDEO zetten voor dit doel een registratiesysteem op. Informatie met rubricering TRÈS SECRET UE/EU TOP SECRET wordt in speciaal daarvoor bestemde registers geregistreerd.
3. De diensten en locaties waar gerubriceerde EU-informatie wordt verwerkt of opgeslagen, worden regelmatig geïnspecteerd door de veiligheidsautoriteit van de EDEO.
4. Gerubriceerde EU-informatie wordt als volgt overgebracht tussen diensten en locaties die zich buiten fysiek beveiligde zones bevinden:
 - a) de algemene regel is dat gerubriceerde EU-informatie wordt overgedragen met elektronische middelen die worden beschermd met encryptieproducten die overeenkomstig artikel 7, lid 5, van dit besluit zijn goedgekeurd, en in overeenstemming met duidelijk vastgestelde operationele beveiligingsprocedures;
 - b) wanneer geen gebruik wordt gemaakt van de onder a) genoemde middelen, wordt gerubriceerde EU-informatie vervoerd:
 - i) op elektronische dragers (zoals usb-sticks, cd's, harde schijven) die worden beschermd met encryptieproducten die overeenkomstig artikel 8, lid 5, van dit besluit zijn goedgekeurd, of
 - ii) in alle overige gevallen, op de wijze die door de veiligheidsautoriteit van de EDEO is voorgeschreven in overeenstemming met de desbetreffende beschermingsmaatregelen in bijlage A III, afdeling V.
5. De bepalingen ter uitvoering van dit artikel zijn in bijlage A III opgenomen.

Artikel 8

Bescherming van gerubriceerde EU-informatie die wordt verwerkt in communicatie- en informatiesystemen

1. „Information assurance” (hierna „IA” genoemd) op het gebied van communicatie- en informatiesystemen is het vertrouwen dat die systemen de erin opgenomen informatie zullen beschermen en zullen functioneren zoals nodig en wanneer nodig, onder de controle van legitieme gebruikers. Doeltreffende IA waarborgt passende niveaus van vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid en authenticiteit. IA is op een risicobeheersingsproces gebaseerd.
2. Een „communicatie- en informatiesysteem” is een systeem waarmee informatie in elektronische vorm kan worden verwerkt. Een communicatie- en informatiesysteem omvat alle functionele bestanddelen die voor het functioneren ervan vereist zijn, waaronder infrastructurele, organisatorische, personele en informatiemiddelen. Deze bijlage is van toepassing op alle communicatie- en informatiesystemen van de EDEO waarmee gerubriceerde EU-informatie wordt verwerkt.
3. Communicatie- en informatiesystemen verwerken gerubriceerde EU-informatie overeenkomstig het IA-concept.
4. Alle communicatie- en informatiesystemen die gerubriceerde EU-informatie verwerken, worden aan een homologatieprocedure onderworpen. Met de homologatie wordt beoogd de verzekering te verkrijgen dat alle toepasselijke beveiligingsmaatregelen zijn getroffen en dat het niveau van bescherming van de gerubriceerde EU-informatie en van het communicatie- en informatiesysteem overeenkomstig dit besluit voldoende wordt geacht. In de homologatieverklaring worden de maximaal toegelaten rubriceringsgraad van de informatie die door een communicatie- en informatiesysteem mag worden verwerkt, en de voorwaarden daarvoor vastgesteld.
5. Communicatie- en informatiesystemen die informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger verwerken, worden zodanig beschermd dat de gerubriceerde informatie niet kan worden gecompromitteerd door onopzettelijke elektromagnetische emissies (hierna „TEMPEST-beveiligingsmaatregelen” genoemd).
6. Wanneer gerubriceerde EU-informatie door encryptieproducten wordt beschermd, worden deze producten goedgekeurd overeenkomstig artikel 8, lid 5, van dit besluit.

7. Tijdens de overdracht van gerubriceerde EU-informatie met elektronische middelen moeten goedgekeurde encryptieproducten worden gebruikt. Niettegenstaande deze eis kunnen specifieke procedures worden toegepast in noodgevallen of in geval van specifieke technische configuraties als bepaald in bijlage A IV.
8. Overeenkomstig artikel 8, lid 6, van dit besluit worden in de mate van het nodige de volgende IA-functies ingesteld:
- a) een IA-autoriteit (hierna „IAA” genoemd);
 - b) een TEMPEST-autoriteit (hierna „TA” genoemd);
 - c) een autoriteit voor de goedkeuring van encryptieproducten (hierna „CAA” genoemd);
 - d) een autoriteit voor de distributie van encryptieproducten (hierna „CDA” genoemd).
9. Overeenkomstig artikel 8, lid 7, van dit besluit worden voor elk systeem ingesteld:
- a) een veiligheidshomologatieautoriteit (hierna „SAA” genoemd);
 - b) een operationele IA-autoriteit.
10. De bepalingen ter uitvoering van dit artikel zijn in bijlage A IV opgenomen.

Artikel 9

Industriële beveiliging

1. Industriële beveiliging is de toepassing van maatregelen om de bescherming van gerubriceerde EU-informatie door contractanten of subcontractanten tijdens precontractuele onderhandelingen en tijdens de volledige looptijd van gerubriceerde opdrachten te waarborgen. De algemene regel is dat in het kader van dergelijke opdrachten geen toegang mag worden verleend tot informatie met rubricering TRÈS SECRET UE/EU TOP SECRET.
2. De EDEO kan opdrachten plaatsen voor taken die toegang tot of verwerking of opslag van gerubriceerde EU-informatie behelzen of vereisen door industriële of andere entiteiten die zijn ingeschreven in een lidstaat of in een derde staat waarmee een informatiebeveiligingsovereenkomst is gesloten of een administratieve regeling als bedoeld in bijlage A, artikel 10, lid 1, is getroffen.
3. De EDEO ziet er als aanbestedende autoriteit op toe dat bij het plaatsen van gerubriceerde opdrachten bij industriële of andere entiteiten aan de in dit besluit en in de gerubriceerde opdrachten vervatte minimumnormen voor industriële beveiliging is voldaan. De EDEO ziet toe op de naleving van dergelijke minimumnormen via de desbetreffende nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit.
4. In een lidstaat geregistreerde contractanten of subcontractanten die deelnemen aan gerubriceerde opdrachten of onderaanneming waarvoor toegang tot of verwerking of opslag van informatie met de rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET binnen hun faciliteiten vereist is, hetzij tijdens de uitvoering van de opdrachten, hetzij in de precontractuele fase, dienen te beschikken over een veiligheidsmachtiging voor een vestiging, die is afgegeven door de nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit of een andere bevoegde veiligheidsautoriteit van de betrokken lidstaat.
5. Personeelsleden van contractanten of subcontractanten die voor de uitvoering van een gerubriceerde opdracht toegang moeten hebben tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, dienen houder te zijn van een veiligheidsmachtiging voor personen die is afgegeven door de desbetreffende nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit of een andere bevoegde veiligheidsautoriteit overeenkomstig de nationale wet- en regelgeving en de minimumbeveiligingsnormen van bijlage A I.
6. De bepalingen ter uitvoering van dit artikel zijn in bijlage A V opgenomen.

Artikel 10

Uitwisseling van gerubriceerde informatie met derde staten en internationale organisaties

1. De EDEO mag gerubriceerde EU-informatie slechts uitwisselen met derde staten of internationale organisaties indien:
- a) tussen de EU en die derde staat of internationale organisatie een informatiebeveiligingsovereenkomst van kracht is die overeenkomstig artikel 37 VEU en artikel 218 VWEU is gesloten, of

- b) tussen de hoge vertegenwoordiger en de bevoegde veiligheidsautoriteiten van die derde staat of internationale organisatie een administratieve regeling van kracht is voor de uitwisseling van informatie die in beginsel geen hogere rubricering dan RESTREINT UE/EU RESTRICTED heeft, die gesloten is overeenkomstig de procedure van artikel 15, lid 5, van dit besluit, of
- c) tussen de EU en die derde staat of internationale organisatie een kader of ad-hocdeelnameovereenkomst in de context van een GVDB-crisisbeheersingsoperatie van toepassing is, die overeenkomstig artikel 37 VEU en artikel 218 VWEU is gesloten,

en aan de voorwaarden van het desbetreffende instrument is voldaan.

Uitzonderingen op deze algemene regel zijn opgenomen in bijlage A VI, afdeling V.

2. De in lid 1, onder b), bedoelde administratieve regelingen bevatten bepalingen om te waarborgen dat, wanneer derde staten of internationale organisaties gerubriceerde EU-informatie ontvangen, die informatie wordt beschermd in overeenstemming met de ervoor geldende rubriceringsgraad en volgens minimumnormen die niet minder streng zijn dan die welke bij dit besluit zijn vastgesteld.

De informatie die wordt uitgewisseld op grond van de overeenkomsten bedoeld in lid 1, onder c), blijft beperkt tot informatie betreffende GVDB-operaties waaraan de betrokken derde staat deelneemt op grond van die overeenkomsten, en in overeenstemming met de bepalingen ervan.

3. Indien vervolgens een informatiebeveiligingsovereenkomst wordt gesloten tussen de Europese Unie en een bijdragende derde staat of internationale organisatie, vervangt de informatiebeveiligingsovereenkomst, wat betreft het uitwisselen en verwerken van gerubriceerde EU-informatie, de bepaling over de uitwisseling van gerubriceerde informatie als neergelegd in een eventuele kaderovereenkomst inzake deelname, ad-hocovereenkomst inzake deelname of administratieve ad-hocregeling.

4. Ten behoeve van een EVDB-operatie gegenereerde gerubriceerde EU-informatie mag worden bekendgemaakt aan personeel dat door derde staten of internationale organisaties bij die operatie gedetacheerd is, overeenkomstig de leden 1-3 en bijlage A VI. Wanneer aan dat personeel toegang tot gerubriceerde EU-informatie wordt verleend in werkruimten of in communicatie- en informatiesystemen van een EVDB-operatie, moeten maatregelen worden getroffen (zoals registratie van bekendgemaakte gerubriceerde EU-informatie) om het risico van verlies of compromittering te verkleinen. Dergelijke maatregelen worden opgesteld in de desbetreffende plannings- of missiedocumenten.

5. Er worden evaluatiebezoeken aan derde staten en internationale organisaties georganiseerd, als bedoeld in artikel 17 van dit besluit, om de doeltreffendheid van de beveiligingsmaatregelen ter bescherming van gerubriceerde EU-informatie te verifiëren.

6. Het besluit tot vrijgave van gerubriceerde EU-informatie die de EDEO onder zich heeft aan een derde staat of een internationale organisatie wordt per geval genomen, naargelang van de aard en de inhoud van die informatie, de noodzaak dat de ontvanger er kennis van neemt en de baat die de EU bij de vrijgave heeft.

Indien een entiteit gerubriceerde informatie heeft verstrekt op basis waarvan de EDEO gerubriceerde EU-informatie heeft opgesteld, verzoekt de EDEO deze entiteit om schriftelijke toestemming, teneinde vast te stellen dat er geen bezwaar tegen vrijgave bestaat.

Indien de gerubriceerde informatie waarvan de vrijgave gewenst wordt, niet afkomstig is van de EDEO, vraagt de EDEO vóór vrijgave schriftelijke toestemming aan de opsteller.

Indien de EDEO echter niet in staat is vast te stellen wie de opsteller is, neemt de veiligheidsautoriteit van de EDEO de verantwoordelijkheid van de opsteller op zich, nadat zij daartoe van de in het Beveiligingscomité van de EDEO vertegenwoordigde lidstaten een unaniem gunstig advies heeft verkregen.

7. De bepalingen ter uitvoering van dit artikel zijn in bijlage A VI opgenomen.

Artikel 11

Inbreuken op de beveiligingsvoorschriften en compromittering van gerubriceerde informatie

1. Elke inbreuk of vermoedelijke inbreuk op de beveiligingsvoorschriften en elke compromittering of vermoedelijke compromittering van gerubriceerde informatie wordt onmiddellijk gemeld aan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, dat naargelang van het geval de betrokken lidstaten dan wel een andere betrokken entiteit inlicht.

2. Wanneer bekend is of er redenen zijn om aan te nemen dat gerubriceerde informatie is gecompromitteerd of verloren is gegaan, licht het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, de nationale veiligheidsautoriteit van de betrokken lidstaat in en neemt het alle passende maatregelen overeenkomstig de relevante wet- en regelgeving, teneinde:

- a) bewijsmateriaal veilig te stellen;
- b) ervoor te zorgen dat de zaak wordt onderzocht door personeel dat niet rechtstreeks met de inbreuk of compromittering te maken heeft, teneinde de feiten vast te stellen;
- c) de opsteller dan wel een andere betrokken entiteit, meteen in te lichten;
- d) herhaling te voorkomen;
- e) de eventuele schade voor de belangen van de EU of de lidstaten te beoordelen, en
- f) de bevoegde instanties in kennis te stellen van de gevolgen van de compromittering of vermoedelijke compromittering en de stappen die zijn ondernomen.

3. Een onder de verantwoordelijkheid van de EDEO geplaatst personeelslid dat verantwoordelijk is voor een inbreuk op de beveiligingsvoorschriften van dit besluit kan aan tuchtmaatregelen worden onderworpen overeenkomstig de geldende regels en voorschriften.

Eenieder die verantwoordelijk is voor de compromittering of het verlies van gerubriceerde informatie kan aan tucht- en/of gerechtelijke maatregelen worden onderworpen overeenkomstig de geldende wet- en regelgeving.

4. Terwijl onderzoek wordt verricht naar de inbreuk en/of compromittering, kan het hoofd van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, de toegang van de betrokkene tot gerubriceerde EU-informatie en tot de locaties van de EDEO intrekken. Het directoraat Beveiliging van het directoraat-generaal Personele Middelen en Veiligheid van de Commissie, de dienst Beveiliging van het secretariaat-generaal van de Raad of de nationale veiligheidsautoriteit van de betrokken lidstaat dan wel andere betrokken entiteit, naargelang van het geval, wordt over een dergelijke beslissing onmiddellijk ingelicht.

BIJLAGE A I

PERSONEELSGERELATEERDE BEVEILIGING

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 5. In deze bijlage worden in het bijzonder de criteria vastgelegd aan de hand waarvan de EDEO bepaalt of aan een persoon, rekening houdend met diens loyaliteit en betrouwbaarheid, toegang tot gerubriceerde EU-informatie mag worden verleend, alsook de onderzoeks- en administratieve procedures die daartoe moeten worden gevolgd.
2. Een „veiligheidsmachtiging voor personen” voor toegang tot gerubriceerde EU-informatie is een verklaring van een bevoegde autoriteit van een lidstaat, die wordt afgegeven na voltooiing van een veiligheidsonderzoek door de bevoegde instanties van die lidstaat, waarin wordt bevestigd dat de betrokkene, mits zijn „noodzaak tot kennisname” is vastgesteld, tot een bepaalde datum toegang kan krijgen tot gerubriceerde EU-informatie tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger); van die persoon wordt dan gezegd dat hij „gecleard” is.
3. Een „certificaat van veiligheidsmachtiging voor personen” is een door de veiligheidsautoriteit van de EDEO afgegeven certificaat waarin wordt bevestigd dat de betrokkene gescreend is en dat de rubriceringsgraad vermeldt van de gerubriceerde EU-informatie waartoe hij toegang kan krijgen, alsook de geldigheidsduur van de veiligheidsmachtiging voor personen en de datum waarop de geldigheid van het certificaat zelf afloopt.
4. Een „machtiging voor toegang tot gerubriceerde EU-informatie” is een machtiging die door de veiligheidsautoriteit van de EDEO overeenkomstig dit besluit wordt verleend nadat de bevoegde instanties van een lidstaat een veiligheidsmachtiging voor personen hebben afgegeven, waarin wordt bevestigd dat de betrokkene, mits zijn „noodzaak tot kennisname” is vastgesteld, tot een bepaalde datum toegang kan krijgen tot gerubriceerde EU-informatie tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger); van die persoon wordt dan gezegd dat hij „gecleard” is.

II. VERLENING VAN TOEGANG TOT GERUBRICEERDE EU-INFORMATIE

5. De toegang tot informatie met rubricering RESTREINT UE/EU RESTRICTED vereist geen veiligheidsmachtiging, en wordt verleend nadat:
 - a) de statutaire of contractuele relatie van de betrokkene met de EDEO is vastgesteld;
 - b) zijn noodzaak tot kennisname is vastgesteld;
 - c) hij is geïnstrueerd over de beveiligingsvoorschriften en -procedures voor de bescherming van gerubriceerde EU-informatie en hij zijn verantwoordelijkheden in verband met de bescherming van gerubriceerde EU-informatie overeenkomstig dit besluit schriftelijk heeft bevestigd.
6. Een persoon wordt alleen toegang tot informatie met rubricering CONFIDENTIEL UE/ EU CONFIDENTIAL of hoger verleend indien:
 - a) de statutaire of contractuele relatie van de betrokkene met de EDEO is vastgesteld;
 - b) zijn noodzaak tot kennisname is vastgesteld;
 - c) hem een veiligheidsmachtiging voor personen voor het passende niveau is verleend of hij anderszins uit hoofde van zijn functie daartoe naar behoren is gemachtigd in overeenstemming met de nationale wet- en regelgeving, en
 - d) hij is geïnstrueerd over de beveiligingsvoorschriften en -procedures voor de bescherming van gerubriceerde EU-informatie en hij zijn verantwoordelijkheden in verband met de bescherming van gerubriceerde EU-informatie schriftelijk heeft bevestigd.
7. De EDEO bepaalt voor welke functies in zijn structuren toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger is vereist en waarvoor derhalve een veiligheidsmachtiging voor personen voor het passende niveau, als bedoeld in punt 4, noodzakelijk is.
8. Personeelsleden van de EDEO moeten opgeven of zij de nationaliteit van meer dan één land bezitten.

Procedures voor verzoeken om een veiligheidsmachtiging voor personen bij de EDEO

9. Voor personeelsleden van de EDEO zendt de veiligheidsautoriteit van de EDEO een ingevulde vragenlijst betreffende de veiligheidsmachtiging voor personen naar de nationale veiligheidsautoriteit van de lidstaat waarvan de betrokkene onderdaan is, met het verzoek een veiligheidsonderzoek uit te voeren voor het niveau van gerubriceerde EU-informatie waartoe de betrokkene toegang moet hebben.
10. Wanneer een persoon het staatsburgerschap van meer dan één land bezit, wordt het screeningverzoek gericht tot de nationale veiligheidsautoriteit van het land waarvan de nationaliteit bepalend was voor de aanwerving van de betrokkene.
11. Wanneer een persoon een veiligheidsmachtiging voor personen heeft aangevraagd, en de EDEO de beschikking krijgt over informatie over de betrokkene die voor het veiligheidsonderzoek relevant is, stelt de EDEO de desbetreffende nationale veiligheidsautoriteit daarvan in kennis overeenkomstig de voorschriften ter zake.
12. Nadat het veiligheidsonderzoek is afgesloten, brengt de betrokken nationale veiligheidsautoriteit het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, op de hoogte van de uitkomst ervan.
 - a) Wanneer het veiligheidsonderzoek tot de zekerheid leidt dat er geen informatie bekend is die doet twijfelen aan de loyaliteit en betrouwbaarheid van de betrokkene, kan de veiligheidsautoriteit van de EDEO de betrokkene een machtiging voor toegang tot gerubriceerde EU-informatie verlenen voor de vereiste rubriceringsgraad, die tot een bepaalde datum geldig is.
 - b) De EDEO neemt alle passende maatregelen om te waarborgen dat de door de nationale veiligheidsautoriteit gestelde voorwaarden of beperkingen daadwerkelijk ten uitvoer worden gelegd. De nationale veiligheidsautoriteit wordt over de resultaten daarvan ingelicht.
 - c) Wanneer het veiligheidsonderzoek niet tot de onder a) bedoelde zekerheid leidt, stelt de veiligheidsautoriteit van de EDEO de betrokkene daarvan in kennis; deze kan vragen om door de veiligheidsautoriteit van de EDEO te worden gehoord. De veiligheidsautoriteit van de EDEO kan de bevoegde nationale veiligheidsautoriteit om elke toelichting vragen die de autoriteit volgens de nationale wet- en regelgeving mag verstrekken. Indien de uitkomst wordt bevestigd, wordt geen machtiging voor toegang tot gerubriceerde EU-informatie verleend. De EDEO neemt in dat geval alle passende maatregelen om te waarborgen dat de betrokkene geen toegang krijgt tot gerubriceerde EU-informatie.
13. Voor het veiligheidsonderzoek en de resultaten daarvan, waarop het besluit van de EDEO tot het al dan niet verlenen van een machtiging voor toegang tot gerubriceerde EU-informatie is gebaseerd, geldt de in de betrokken lidstaat van toepassing zijnde wet- en regelgeving, ook wat de mogelijkheden tot beroep betreft. Tegen besluiten van de veiligheidsautoriteit van de EDEO kan beroep worden ingesteld in overeenstemming met het Statuut.
14. De zekerheid waarop een veiligheidsmachtiging voor personen gebaseerd is, op voorwaarde dat de machtiging geldig blijft, strekt zich uit tot elke taak die de betrokkene bij de EDEO, het secretariaat-generaal van de Raad of de Commissie op zich neemt.
15. De EDEO aanvaardt de door een andere instelling, een ander orgaan of agentschap van de Europese Unie verleende machtiging voor toegang tot gerubriceerde EU-informatie, op voorwaarde dat de machtiging geldig blijft. De machtiging bestrijkt elke taak die de betrokkene binnen de EDEO op zich neemt. De instelling, het orgaan of agentschap van de Europese Unie waar de betrokkene in dienst treedt, geeft de bevoegde nationale veiligheidsautoriteit kennis van de wijziging van werkgever.
16. Indien het dienstverband van een persoon niet begint binnen twaalf maanden na de kennisgeving van de uitkomst van het veiligheidsonderzoek aan de veiligheidsautoriteit van de EDEO, of indien de betrokkene zijn dienst voor een periode van twaalf maanden heeft onderbroken en gedurende die tijd niet heeft gewerkt bij de EDEO, bij andere instellingen, organen of instanties van de EU of in een functie bij een nationale overheid van een lidstaat waarvoor toegang tot gerubriceerde informatie is vereist, wordt de betrokken nationale veiligheidsautoriteit verzocht te bevestigen dat de uitkomst van het veiligheidsonderzoek nog steeds geldig en correct is.
17. Wanneer een persoon een geldige veiligheidsmachtiging voor personen heeft, en de EDEO de beschikking krijgt over informatie dat er in verband met die persoon een veiligheidsrisico bestaat, stelt de EDEO de desbetreffende nationale veiligheidsautoriteit daarvan in kennis overeenkomstig de voorschriften ter zake en kan hij de toegang tot gerubriceerde EU-informatie opschorten of de machtiging voor toegang tot gerubriceerde EU-informatie intrekken. Wanneer een nationale veiligheidsautoriteit de EDEO in kennis stelt van de intrekking van een overeenkomstig punt 12, onder a), gegeven zekerheid voor een persoon die een geldige machtiging voor toegang tot gerubriceerde EU-informatie heeft, kan de veiligheidsautoriteit van de EDEO de nationale veiligheidsautoriteit om elke toelichting vragen die de autoriteit volgen de nationale wet- en regelgeving mag verstrekken. Indien de negatieve informatie wordt bevestigd, wordt de genoemde machtiging ingetrokken en wordt de betrokkene de toegang ontegensprekend tot gerubriceerde EU-informatie en tot functies waar dergelijke toegang mogelijk is of waar hij de veiligheid in gevaar zou kunnen brengen.

18. Elke beslissing om een machtiging voor toegang tot gerubriceerde EU-informatie van een personeelslid van de EDEO in te trekken, alsmede de redenen daarvoor, indien gepast, wordt meegedeeld aan de betrokkene, die kan verzoeken om door de veiligheidsautoriteit van de EDEO te worden gehoord. Voor door een nationale veiligheidsautoriteit verstrekte informatie geldt de in de betrokken lidstaat van toepassing zijnde wet- en regelgeving, ook wat de mogelijkheden tot beroep betreft. Tegen besluiten van de veiligheidsautoriteit van de EDEO kan beroep worden ingesteld in overeenstemming met het Statuut.
19. Nationale deskundigen die bij de EDEO worden gedetacheerd in een functie waarvoor toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger is vereist, dienen aan de veiligheidsautoriteit van de EDEO een geldige nationale veiligheidsmachtiging voor personen voor toegang tot gerubriceerde EU-informatie met de juiste rubriceringsgraad over te leggen, alvorens hun taak aan te vatten. Dit proces wordt beheerd door de uitzendende lidstaat.

Registratie van veiligheidsmachtigingen voor personen

20. De EDEO houdt een database bij van de veiligheidsmachtigingsstatus van alle onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden en personeelsleden van contractanten van de EDEO. In deze database worden het niveau van de gerubriceerde EU-informatie waartoe een persoon toegang kan worden verleend (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), de datum van verlening van de veiligheidsmachtiging en de geldigheidsduur ervan geregistreerd.
21. In samenwerking met de lidstaten en andere instellingen, organen en instanties van de EU worden passende coördinatieprocedures ingesteld om te waarborgen dat de EDEO kan beschikken over een nauwkeurig en volledig beeld van de veiligheidsmachtigingsstatus van alle onder de verantwoordelijkheid van de EDEO geplaatste personeelsleden en personeelsleden van contractanten van de EDEO.
22. De veiligheidsautoriteit van de EDEO kan een certificaat van veiligheidsmachtiging voor personen afgeven met vermelding van het niveau van de gerubriceerde EU-informatie waartoe de persoon toegang kan worden verleend (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), de geldigheidsduur van de betrokken veiligheidsmachtiging voor personen of machtiging en de datum waarop de geldigheid van het certificaat zelf afloopt.

Vrijstellingen van de eis inzake veiligheidsmachtiging voor personen

23. Personen die overeenkomstig de nationale wet- en regelgeving uit hoofde van hun functie gemachtigd zijn om toegang te krijgen tot gerubriceerde EU-informatie, worden door het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, geïnstrueerd over hun beveiligingsverplichtingen in verband met de bescherming van gerubriceerde EU-informatie.

III. VEILIGHEIDSOPLEIDING EN VEILIGHEIDSBESEF

24. Voordat een persoon wordt gemachtigd om toegang te krijgen tot gerubriceerde EU-informatie, dient deze schriftelijk te bevestigen dat hij op de hoogte is van zijn plichten met betrekking tot de bescherming van gerubriceerde EU-informatie en van de gevolgen indien gerubriceerde EU-informatie wordt gecompromitteerd. Een aantekening van deze schriftelijke bevestiging wordt door de EDEO bewaard.
25. Eenieder die gemachtigd is om toegang te krijgen tot gerubriceerde EU-informatie of deze moet verwerken, wordt vanaf het begin bewust gemaakt van en regelmatig geïnstrueerd over bedreigingen voor de veiligheid en moet iedere toenadering of activiteit die hij verdacht of ongewoon acht, onmiddellijk aan de desbetreffende veiligheidsautoriteiten melden.
26. Eenieder die toegang heeft tot gerubriceerde EU-informatie, wordt onderworpen aan voortdurende persoonsgerelateerde beveiligingsmaatregelen (nazorg) zolang hij gerubriceerde EU-informatie verwerkt. Deze voortdurende persoonsgerelateerde beveiliging behoort tot de verantwoordelijkheid van:
 - a) personen die toegang hebben tot gerubriceerde EU-informatie: eenieder is persoonlijk verantwoordelijk voor zijn eigen veiligheidsgerelateerd gedrag en dient iedere toenadering of activiteit die hij verdacht of ongewoon vindt, onmiddellijk te melden aan de desbetreffende veiligheidsinstanties, alsmede elke verandering in zijn persoonlijke omstandigheden die van invloed kan zijn op zijn veiligheidsmachtiging of machtiging voor toegang tot gerubriceerde EU-informatie;
 - b) leidinggevend: zij moeten erop toezien dat hun personeelsleden bekend zijn met de veiligheidsmaatregelen en verantwoordelijkheden met betrekking tot de bescherming van gerubriceerde EU-informatie en dat het veiligheidsgedrag van hun personeelsleden in het oog wordt gehouden; zij dienen elk beveiligingsprobleem van enige betekenis hetzij zelf aan te pakken, hetzij alle negatieve informatie die van invloed kan zijn op de veiligheidsmachtigingen of machtigingen voor toegang tot gerubriceerde EU-informatie van hun personeelsleden te melden aan de passende veiligheidsautoriteiten;

- c) actoren van de veiligheidsorganisatie van de EDEO, bedoeld in artikel 12 van dit besluit: zij zijn verantwoordelijk voor het geven van briefings op het gebied van beveiligingsvoorlichting en zien erop toe dat alle personeelsleden binnen hun gebied regelmatig worden geïnstrueerd; zij stimuleren een solide veiligheidscultuur binnen hun verantwoordelijkheidsgebied en stellen maatregelen in voor de monitoring van het veiligheidsgedrag van het personeel en voor het melden aan de bevoegde veiligheidsautoriteiten van alle negatieve informatie die van invloed kan zijn op iemands veiligheidsmachtiging;
 - d) de EDEO en lidstaten: zij zorgen voor de noodzakelijke kanalen voor het doorgeven van informatie die gevolgen kan hebben voor iemands veiligheidsmachtiging of machtiging voor toegang tot gerubriceerde EU-informatie.
27. Alle personen die geen taken meer vervullen waarvoor toegang tot gerubriceerde EU-informatie vereist is, dienen er bewust van te worden gemaakt dat hun plichten met betrekking tot de bescherming van gerubriceerde EU-informatie blijven bestaan, en dienen zulks in voorkomend geval schriftelijk te bevestigen.

IV. UITZONDERLIJKE OMSTANDIGHEDEN

28. De veiligheidsautoriteit van de EDEO kan om dringende en naar behoren gemotiveerde redenen van dienstbelang en in afwachting van de voltooiing van het volledige veiligheidsonderzoek, na raadpleging van de nationale veiligheidsautoriteit van de lidstaat waarvan de betrokkene onderdaan is en afhankelijk van de uitkomst van een eerste controle of er geen negatieve informatie bekend is, ambtenaren en andere personeelsleden van de EDEO voor een specifieke functie tijdelijk toegang tot gerubriceerde EU-informatie verlenen. Er dient zo spoedig mogelijk een volledig veiligheidsonderzoek te worden verricht. Tijdelijke toegang wordt voor ten hoogste zes maanden verleend en geldt niet voor informatie met rubricering TRÈS SECRET UE/EU TOP SECRET. Alle personen aan wie tijdelijke toegang is verleend, bevestigen schriftelijk dat zij kennis dragen van hun plichten met betrekking tot de bescherming van gerubriceerde EU-informatie en van de gevolgen indien gerubriceerde EU-informatie wordt gecompromitteerd. Een aantekening van deze schriftelijke bevestiging wordt door de EDEO bewaard.
29. Wanneer een persoon een functie krijgt toegewezen waarvoor een veiligheidsmachtiging voor personen nodig is van één niveau hoger dan die waarover hij op dat moment beschikt, kan deze nieuwe functie op voorlopige basis worden toegewezen, mits:
- a) de dwingende noodzaak van toegang tot gerubriceerde EU-informatie met een hogere rubriceringsgraad schriftelijk door de hiërarchische meerdere van de betrokkene wordt bevestigd;
 - b) de toegang wordt beperkt tot specifieke onderdelen van de gerubriceerde EU-informatie die nodig zijn voor de functie;
 - c) de persoon in het bezit is van een geldige veiligheidsmachtiging;
 - d) er stappen zijn ondernomen om machtiging voor het voor de functie vereiste toegangsniveau te verkrijgen;
 - e) uit controles door de bevoegde autoriteit genoegzaam is gebleken dat de betrokkene de beveiligingsvoorschriften niet ernstig of herhaaldelijk heeft overtreden;
 - f) de toewijzing van de functie aan de betrokkene is goedgekeurd door de bevoegde autoriteit van de EDEO;
 - g) de betrokken nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit die de veiligheidsmachtiging van de betrokkene heeft afgegeven, is geraadpleegd en deze geen bezwaren heeft geuit, en
 - h) een aantekening van de verleende uitzondering, met inbegrip van een beschrijving van de informatie waartoe toegang werd verleend, wordt bewaard door het verantwoordelijke register of subregister.
30. Deze procedure wordt gebruikt voor eenmalige toegang tot gerubriceerde EU-informatie met een rubriceringsgraad die één niveau hoger ligt dan waarvoor de betrokkene is gescreend. Deze procedure mag niet bij herhaling worden gebruikt.
31. In zeer uitzonderlijke omstandigheden, zoals bij missies in een vijandige omgeving of gedurende perioden van toenemende internationale spanning, wanneer noodmaatregelen zulks vereisen, in het bijzonder wanneer er levens kunnen worden gered, kan de hoge vertegenwoordiger, de veiligheidsautoriteit van de EDEO of de directeur-generaal begroting en administratie schriftelijk toegang verlenen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET aan personen die niet in het bezit zijn van de vereiste veiligheidsmachtiging voor personen, zulks op voorwaarde dat die toestemming absoluut noodzakelijk is. Een aantekening van deze toestemming, met een beschrijving van de informatie waartoe toegang werd verleend, wordt bewaard.

32. In geval van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET dienen dergelijke noodmaatregelen beperkt te blijven tot onderdanen van de Europese Unie aan wie toegang is verleend tot het nationale equivalent van TRÈS SECRET UE/EU TOP SECRET of tot informatie met rubricering SECRET UE/EU SECRET.
33. Het Beveiligingscomité van de EDEO moet op de hoogte worden gesteld van gevallen waarin de in de punten 31 en 32 genoemde procedure is gevolgd.
34. Aan het Beveiligingscomité van de EDEO moet jaarlijks verslag worden uitgebracht over het gebruik van de in deze afdeling beschreven procedures.

V. BIJWONEN VAN VERGADERINGEN OP HET HOOFDKANTOOR VAN DE EDEO EN DE DELEGATIES VAN DE UNIE

35. Personen aan wie is opgedragen deel te nemen aan vergaderingen op het hoofdkantoor van de EDEO of delegaties van de Unie waarin informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt besproken, doen zulks uitsluitend indien de veiligheidsmachtigingsstatus van de betrokkene is bevestigd. Voor vertegenwoordigers van de lidstaten, ambtenaren van het secretariaat-generaal van de Raad en de Commissie wordt een certificaat van veiligheidsmachtiging voor personen of een ander bewijs van een veiligheidsmachtiging voor personen door de desbetreffende autoriteiten toegezonden aan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, of de veiligheidscoördinator van de delegatie van de Unie, of in uitzonderingsgevallen door de betrokkene overgelegd. Indien van toepassing kan een geconsolideerde lijst van namen worden gebruikt, met het relevante bewijs van de veiligheidsmachtiging voor personen.
36. Wanneer de veiligheidsmachtiging voor toegang tot gerubriceerde EU-informatie wordt ingetrokken van een persoon die voor zijn werkzaamheden moet deelnemen aan vergaderingen op het hoofdkantoor van de EDEO of delegaties van de Unie waarin informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger wordt besproken, licht de bevoegde autoriteit de EDEO daarover in.

VI. MOGELIJKE TOEGANG TOT GERUBRICEERDE EU-INFORMATIE

37. Wanneer personen moeten werken in omstandigheden waarin zij mogelijktoegang hebben tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger, dienen zij passend te zijn gemachtigd of voortdurend te worden begeleid.
38. Koeriers en bewakings- en begeleidingspersoneel dienen voor de passende rubriceringsgraad te zijn gemachtigd of anderszins een passend onderzoek te hebben ondergaan overeenkomstig de nationale wet- en regelgeving, regelmatig te worden geïnstrueerd over de beveiligingsprocedures ter bescherming van gerubriceerde EU-informatie en over hun plicht om gerubriceerde EU-informatie te beschermen die hun is toevertrouwd of waartoe zij onbedoeld toegang kunnen hebben gekregen.

BIJLAGE A II

FYSIEKE BEVEILIGING VAN GERUBRICEERDE EU-INFORMATIE

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 6. In deze bijlage worden minimumvoorschriften vastgesteld voor de fysieke beveiliging van locaties, gebouwen, kantoren, ruimten en andere zones waar gerubriceerde EU-informatie wordt verwerkt en opgeslagen, met inbegrip van zones waar communicatie- en informatiesystemen zijn ondergebracht.
2. Fysieke beveiligingsmaatregelen zijn bedoeld om de toegang zonder machtiging tot gerubriceerde EU-informatie te voorkomen door:
 - a) ervoor te zorgen dat gerubriceerde EU-informatie op passende wijze wordt behandeld en opgeslagen;
 - b) op basis van het „noodzaak tot kennisname”-beginsel en, in voorkomend geval, van hun veiligheidsmachtiging een onderscheid tussen personeelsleden mogelijk te maken wat de toegang tot gerubriceerde EU-informatie betreft;
 - c) acties waarvoor geen toestemming is verleend af te schrikken, tegen te houden en op te sporen, en
 - d) het door list of geweld binnendringen te verhinderen of te vertragen.

II. VEREISTEN EN MAATREGELEN INZAKE FYSIEKE BEVEILIGING

3. De EDEO past een risicobeheersingsproces toe ter bescherming van gerubriceerde EU-informatie op zijn locaties, teneinde ervoor te zorgen dat een fysieke bescherming wordt geboden die overeenstemt met het ingeschatte risico. In het risicobeheersingsproces wordt rekening gehouden met alle relevante factoren, met name:
 - a) de rubriceringsgraad van de gerubriceerde EU-informatie;
 - b) de vorm en omvang van de gerubriceerde EU-informatie, waarbij in aanmerking moet worden genomen dat grote hoeveelheden of een compilatie van gerubriceerde EU-informatie de toepassing van strengere beschermingsmaatregelen kunnen vergen;
 - c) de omgeving en de structuur van de gebouwen of zones waar gerubriceerde EU-informatie is ondergebracht;
 - d) de dreigingsevaluatie in verband met derde landen die door INTCEN is verricht op basis van met name de rapportage van de delegaties van de Unie, en
 - e) de beoordeelde dreiging die uitgaat van inlichtingendiensten die zich richten op de Europese Unie of de lidstaten en van sabotage, terrorisme en subversie of andere criminele activiteiten.
4. De veiligheidsautoriteit van de EDEO stelt aan de hand van het begrip „defence in depth” vast welke passende combinatie van fysieke beveiligingsmaatregelen moet worden getroffen. Deze maatregelen kunnen zijn:
 - a) een afsluiting: een fysieke barrière ter verdediging van de grens van een zone die bescherming behoeft;
 - b) indringerdetectiesystemen (hierna „IDS” genoemd): een IDS kan worden gebruikt om het beveiligingsniveau van de afsluiting te verhogen, of in lokalen en gebouwen om beveiligingspersoneel te vervangen of te ondersteunen;
 - c) toegangscontrole: er kan toegangscontrole worden uitgeoefend voor een locatie, een gebouw of gebouwen op een locatie of voor zones of ruimten in een gebouw. De controle kan elektronisch of elektromechanisch worden verricht, door beveiligingspersoneel en/of een receptionist, of met enig ander fysiek hulpmiddel;
 - d) beveiligingspersoneel: beveiligingspersoneel dat een opleiding heeft gekregen, onder toezicht werkt en, in voorkomend geval, een gedegen veiligheidsonderzoek heeft ondergaan, kan onder meer worden ingezet om personen af te schrikken die overwegen heimelijk binnen te dringen;
 - e) gesloten tv-circuit: een gesloten tv-circuit kan door beveiligingspersoneel worden gebruikt om incidenten en IDS-alarmen op grote locaties of aan de afsluitingen te controleren;

- f) beveiligingsverlichting: beveiligingsverlichting kan worden gebruikt om mogelijke indringers af te schrikken en biedt daarnaast de noodzakelijke verlichting voor effectieve bewaking die rechtstreeks door beveiligingspersoneel dan wel onrechtstreeks via een gesloten tv-circuit geschiedt, en
 - g) alle andere passende fysieke maatregelen om ongeoorloofde toegang te ontmoedigen of op te sporen of om verlies of beschadiging van gerubriceerde EU-informatie te voorkomen.
- 5. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, mag controles uitvoeren bij het binnen- en buitengaan, ter afschrikking van het ongeoorloofd binnenbrengen van materiaal in, of het ongeoorloofd verwijderen van gerubriceerde EU-informatie uit een locatie of gebouw.
 - 6. Als het risico bestaat dat gerubriceerde EU-informatie van buitenaf wordt gezien, zelfs per ongeluk, worden passende maatregelen genomen om dit risico te voorkomen.
 - 7. Voor nieuwe voorzieningen worden fysieke beveiligingsvereisten en functiespecificaties reeds bij het plannen en ontwerpen vastgesteld. Voor bestaande voorzieningen worden fysieke beveiligingsvereisten zo veel mogelijk uitgevoerd.

III. UITRUSTING VOOR DE FYSIEKE BESCHERMING VAN GERUBRICEERDE EU-INFORMATIE

- 8. Bij de aanschaf van uitrusting (zoals beveiligde opbergmiddelen, papierversnipperaars, deursloten, elektronische systemen voor toegangscontrole, indringerdetectiesystemen, alarmsystemen) voor de fysieke bescherming van gerubriceerde EU-informatie ziet de veiligheidsautoriteit van de EDEO erop toe dat de uitrusting in overeenstemming is met de goedgekeurde technische normen en minimumvoorschriften.
- 9. De technische specificaties van uitrusting die bestemd is voor de fysieke bescherming van gerubriceerde EU-informatie worden vastgelegd in beveiligingsrichtsnoeren die door het Beveiligingscomité van de EDEO moeten worden goedgekeurd.
- 10. De beveiligingssystemen worden geregeld geïnspecteerd en de uitrusting wordt regelmatig onderhouden. Bij de onderhoudswerkzaamheden wordt met het resultaat van de inspecties rekening gehouden om te garanderen dat de uitrusting optimaal blijft werken.
- 11. De effectiviteit van individuele beveiligingsmaatregelen en van het gehele beveiligingssysteem wordt bij iedere inspectie getoetst.

IV. FYSIEKE BESCHERMDE ZONES

- 12. Voor de fysieke bescherming van gerubriceerde EU-informatie worden twee soorten fysiek beschermde zones, of de nationale equivalenten ervan, ingesteld:
 - a) administratieve zones, en
 - b) beveiligde zones (waaronder technisch beveiligde zones).
- 13. De veiligheidsautoriteit van de EDEO bepaalt dat een zone voldoet aan de eisen om te worden aangewezen als administratieve zone, beveiligde zone of technisch beveiligde zone.
- 14. Voor administratieve zones:
 - a) wordt een duidelijk omschreven afscheiding ingesteld waar personen en indien mogelijk voertuigen kunnen worden gecontroleerd;
 - b) wordt toegang zonder begeleiding alleen toegestaan aan personen die naar behoren door het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, gemachtigd zijn, en
 - c) worden alle andere personen altijd begeleid of aan gelijkwaardige controles onderworpen.
- 15. Voor beveiligde zones:
 - a) wordt een duidelijk omschreven, beschermde afscheiding ingesteld waar elk binnen- en buitengaan wordt gecontroleerd door middel van een systeem met toegangspasjes of persoonsherkenning;

- b) wordt toegang zonder begeleiding alleen verleend aan personen die een veiligheidsonderzoek op het vereiste niveau hebben ondergaan en specifiek gemachtigd zijn om de zone te betreden op basis van hun noodzaak tot kennisname;
 - c) worden alle andere personen altijd begeleid of aan gelijkwaardige controles onderworpen.
16. Wanneer het betreden van een beveiligde zone in de praktijk neerkomt op rechtstreekse toegang tot de gerubriceerde informatie die zich daar bevindt, zijn daarnaast de volgende aanvullende voorschriften van toepassing:
- a) de hoogste rubriceringsgraad van de informatie die normaal in de zone worden bewaard, wordt duidelijk aangegeven;
 - b) alle bezoekers moeten een specifieke machtiging bezitten om de zone te betreden, moeten altijd worden begeleid en moeten passend gemachtigd zijn, tenzij het nodig wordt gedaan om toegang tot gerubriceerde EU-informatie onmogelijk te maken;
 - c) elektronische apparatuur moet buiten de zone worden achtergelaten.
17. Beveiligde zones die tegen af luisteren zijn beschermd, worden als technisch beveiligde zones aangemerkt. Daarnaast zijn de volgende aanvullende voorschriften van toepassing:
- a) de zones worden uitgerust met een IDS, worden afgesloten wanneer ze niet worden gebruikt en bewaakt wanneer ze in gebruik zijn. Sleutels worden gecontroleerd overeenkomstig afdeling VI van deze bijlage;
 - b) alle personen en goederen die deze zones binnenkomen, worden gecontroleerd;
 - c) deze zones worden aan regelmatige fysieke en/of technische inspecties onderworpen, zoals vereist door de veiligheidsautoriteit van de EDEO. Die inspecties worden ook verricht nadat de zones door onbevoegden zijn betreden of indien dit wordt vermoed, en
 - d) deze zones zijn vrij van ongeoorloofde communicatielijnen of telefoons of andere ongeoorloofde communicatie-apparatuur en elektrische of elektronische apparatuur.
18. Niettegenstaande punt 17, onder d), moet communicatieapparatuur en elektrische en elektronische apparatuur van welke aard ook, voordat zij wordt gebruikt in zones waar vergaderingen plaatsvinden of werkzaamheden worden verricht in verband met informatie met rubricering SECRET UE/EU SECRET en hoger, wanneer de dreiging voor gerubriceerde EU-informatie als hoog wordt beoordeeld, eerst door de veiligheidsautoriteit van de EDEO worden onderzocht om te waarborgen dat geen begrijpelijke informatie door die apparatuur onbedoeld of op illegale wijze over de afscheiding van de betrokken beveiligde zone heen kan worden doorgegeven.
19. Beveiligde zones waar niet op 24-uursbasis dienstdoend personeel aanwezig is, worden, in voorkomend geval, aan het eind van de normale werktijd geïnspecteerd, alsook buiten de normale werktijd met willekeurige tussenpozen, tenzij er een IDS is.
20. Beveiligde zones en technische beveiligde zones kunnen binnen een administratieve zone tijdelijk worden ingesteld voor een gerubriceerde vergadering of een soortgelijk doel.
21. Voor iedere beveiligde zone worden operationele beveiligingsprocedures opgesteld, waarbij het volgende wordt vastgesteld:
- a) het niveau van de gerubriceerde EU-informatie die in die zone mag worden behandeld en opgeslagen;
 - b) de te handhaven bewakings- en beschermingsmaatregelen;
 - c) de personen die op grond van hun noodzaak tot kennisname en veiligheidsmachtiging zonder begeleiding toegang mogen hebben tot de zone;
 - d) in voorkomend geval, de procedures inzake begeleiding of inzake bescherming van gerubriceerde EU-informatie wanneer aan anderen toegang tot de zone wordt verleend;
 - e) andere relevante maatregelen en procedures.
22. Binnen de beveiligde zones worden kluizen geïnstalleerd. De muren, vloeren, plafonds, ramen en afsluitbare deuren moeten door de veiligheidsautoriteit van de EDEO worden goedgekeurd en een gelijkwaardig beschermingsniveau bieden als de beveiligde opbergmiddelen die zijn goedgekeurd voor de opslag van gerubriceerde EU-informatie met dezelfde rubriceringsgraad.

V. FYSIEKE BEVEILIGINGSMAATREGELEN VOOR HET BEHANDELEN EN OPSLAAN VAN GERUBRICEERDE EU-INFORMATIE

23. Gerubriceerde EU-informatie met rubricering RESTREINT UE/EU RESTRICTED mag worden behandeld:

- a) in een beveiligde zone;
- b) in een administratieve zone, als de gerubriceerde EU-informatie wordt beschermd tegen toegang door onbevoegden, of
- c) buiten een beveiligde of een administratieve zone, als de houder de gerubriceerde EU-informatie vervoert overeenkomstig bijlage A III, punten 30 tot en met 42, en zich heeft verbonden tot inachtneming van de in de beveiligingsinstructies van de veiligheidsautoriteit van de EDEO opgenomen compenserende maatregelen ter bescherming van gerubriceerde EU-informatie tegen toegang door onbevoegden.

24. Gerubriceerde EU-informatie met rubricering RESTREINT UE/EU RESTRICTED wordt opgeslagen in daarvoor geschikt afgesloten kantoormeubilair in een administratieve zone of een beveiligde zone. De informatie mag tijdelijk buiten een beveiligde of een administratieve zone worden opgeslagen, als de houder zich heeft verbonden tot inachtneming van de compenserende maatregelen volgens de beveiligingsinstructies van de veiligheidsautoriteit.

25. Gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/ EU SECRET mag worden behandeld:

- a) in een beveiligde zone;
- b) in een administratieve zone, als de gerubriceerde EU-informatie wordt beschermd tegen toegang door onbevoegden, of
- c) buiten een beveiligde zone of een administratieve zone als de houder:
 - i) de gerubriceerde EU-informatie vervoert overeenkomstig bijlage A III, punten 30 tot en met 42;
 - ii) zich heeft verbonden tot inachtneming van de in de beveiligingsinstructies van de bevoegde veiligheidsautoriteit opgenomen compenserende maatregelen ter bescherming van gerubriceerde EU-informatie tegen toegang door onbevoegden;
 - iii) de gerubriceerde EU-informatie te allen tijde onder zijn persoonlijke controle houdt, en
 - iv) in het geval van documenten op papier, het desbetreffend register op de hoogte heeft gebracht.

26. Gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/ EU SECRET wordt in een beveiligde zone opgeslagen in een beveiligingsopbergmiddel of in een kluis.

27. Gerubriceerde EU-informatie met rubricering TRÈS SECRET UE/EU TOP SECRET wordt behandeld in een beveiligde zone.

28. Gerubriceerde EU-informatie met rubricering TRÈS SECRET UE/EU TOP SECRET wordt opgeslagen in een beveiligde zone, op één van de volgende manieren:

- a) in een beveiligd opbergmiddel dat voldoet aan punt 8, met één of meer van de volgende aanvullende controle-middelen:
 - i) voortdurende bescherming of verificatie door beveiligingspersoneel of dienstdoend personeel in het bezit van een veiligheidsmachtiging;
 - ii) een goedgekeurd IDS in combinatie met interventiebeveiligingspersoneel;of
- b) in een met een IDS uitgeruste kluis in combinatie met interventiebeveiligingspersoneel.

29. De voorschriften voor het vervoeren van gerubriceerde EU-informatie buiten fysiek beveiligde zones zijn opgenomen in bijlage A III.

VI. CONTROLE VAN SLEUTELS EN CODECOMBINATIES DIE WORDEN GEBRUIKT VOOR DE BESCHERMING VAN GERUBRICEERDE EU-INFORMATIE

30. De veiligheidsautoriteit van de EDEO stelt procedures vast voor het beheer van sleutels en codecombinaties voor kantoren, lokalen, kluisen en beveiligde opbergmiddelen. Die procedures moeten bescherming bieden tegen ongeoorloofde toegang.

31. De codecombinaties worden gememoriseerd door zo weinig mogelijk personen die er kennis van moeten nemen. De codecombinaties van beveiligde opbergmiddelen en kluizen waarin gerubriceerde EU-informatie wordt opgeslagen, worden gewijzigd:
- a) bij ontvangst van nieuwe opbergmiddelen;
 - b) in geval van een wijziging in het personeel dat de combinatie kent;
 - c) na compromittering of het vermoeden daarvan;
 - d) wanneer een slot in onderhoud of in herstelling is geweest, en
 - e) ten minste om de 12 maanden.
-

BIJLAGE A III

BEHEER VAN GERUBRICEERDE INFORMATIE**I. INLEIDING**

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 7. Zij stelt de administratieve maatregelen vast voor het controleren van gerubriceerde EU-informatie gedurende de gehele levenscyclus ervan, teneinde al dan niet opzettelijke compromittering of verlies van die informatie te helpen voorkomen, opsporen en herstellen.

II. RUBRICERINGSBEHEER**Rubriceringen en markeringen**

2. Informatie wordt gerubriceerd wanneer zij bescherming behoeft wat de vertrouwelijkheid ervan betreft.
3. De opsteller van gerubriceerde EU-informatie is verantwoordelijk voor het bepalen van de rubriceringsgraad, overeenkomstig de desbetreffende rubriceringsrichtsnoeren, en voor de verspreiding van de informatie.
4. De rubriceringsgraad wordt vastgesteld overeenkomstig bijlage A, artikel 2, lid 2, en onder verwijzing naar de beveiligingsrichtsnoeren die overeenkomstig bijlage A, artikel 3, lid 3, moeten worden vastgesteld.
5. Voor gerubriceerde informatie van de lidstaten die met de EDEO wordt uitgewisseld, geldt hetzelfde beschermingsniveau als voor gerubriceerde EU-informatie met een gelijkwaardige rubricering. Een concordantietabel voor de rubriceringen is opgenomen in aanhangsel B van dit besluit.
6. De rubricering, alsmede in voorkomend geval de datum of de specifieke gebeurtenis waarna de informatie lager gerubriceerd of gederubriceerd kan worden, wordt duidelijk en correct aangegeven, ongeacht of de gerubriceerde EU-informatie in papieren, mondelinge, elektronische of andere vorm bestaat.
7. Afzonderlijke delen van een bepaald document (zoals bladzijden, punten, afdelingen, bijlagen, aanhangsels, bijlagen of bijvoegsels) kunnen verschillende rubriceringen vereisen en worden dienovereenkomstig gemarkeerd, ook wanneer zij elektronisch worden opgeslagen.
8. Voor zover mogelijk worden documenten die delen met verschillende rubriceringsgraden bevatten, zo gestructureerd dat de delen met een verschillende rubriceringsgraad gemakkelijk kunnen worden herkend en, indien nodig, worden gescheiden.
9. De rubricering die voor het gehele document of bestand geldt, is van ten minste dezelfde graad als die van het hoogst gerubriceerde gedeelte ervan. Wanneer informatie uit diverse bronnen wordt verzameld, wordt voor het eindproduct in zijn geheel nagegaan welke rubriceringsgraad het moet krijgen, aangezien hiervoor een hogere rubricering vereist kan zijn dan voor de onderdelen ervan.
10. De rubricering van een brief of een nota bij bijvoegsels is van dezelfde graad als het hoogst gerubriceerde bijvoegsel. De opsteller geeft door middel van een passende markering duidelijk aan welke rubricering op de brief of nota moet worden toegepast indien deze gescheiden wordt van de bijvoegsels, bijvoorbeeld:

CONFIDENTIEL UE/EU CONFIDENTIAL

Zonder bijlage(n): RESTREINT UE/EU RESTRICTED

Markeringen

11. Ter aanvulling van een van de rubriceringen als bedoeld in bijlage A, artikel 2, lid 2, kan gerubriceerde EU-informatie voorzien zijn van aanvullende markeringen zoals:
 - a) een identificatiemiddel om de opsteller aan te duiden;
 - b) waarschuwingsmarkeringen, codewoorden of afkortingen waarmee het activiteitengebied waarop het document betrekking heeft, een speciale verspreiding op basis van noodzaak tot kennisname of beperkingen voor het gebruik worden aangegeven;
 - c) markeringen inzake de geschiktheid voor vrijgave.

12. Nadat is besloten tot vrijgave van gerubriceerde EU-informatie aan een derde staat of internationale organisatie, verzendt het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, de betrokken gerubriceerde informatie met daarop een markering inzake de geschiktheid voor vrijgave die vermeldt aan welke derde staat of internationale organisatie de informatie wordt vrijgegeven.
13. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, stelt een lijst van toegestane markeringen vast.

Afgekorte rubriceringsmarkeringen

14. Gestandaardiseerde afgekorte rubriceringsmarkeringen kunnen worden gebruikt om de rubriceringsgraad van afzonderlijke delen van een tekst aan te geven. Afkortingen komen niet in de plaats van de volledige rubricerings-aanduidingen.
15. De volgende standaardafkortingen mogen in gerubriceerde EU-documenten worden gebruikt ter aanduiding van de rubriceringsgraad van afdelingen of onderdelen van tekst van minder dan één bladzijde:

TRÈS SECRET UE/EU TOP SECRET
SECRET UE/EU SECRET
CONFIDENTIEL UE/EU CONFIDENTIAL
RESTREINT UE/EU RESTRICTED

TS-UE/EU-TS
S-UE/EU-S
C-UE/EU-C
R-UE/EU-R

Genereren van gerubriceerde EU-informatie

16. Bij het genereren van een gerubriceerd EU-document:
 - a) wordt op elke bladzijde duidelijk de rubriceringsgraad aangegeven;
 - b) wordt elke bladzijde genummerd;
 - c) wordt het document voorzien van een referentienummer en een onderwerp, dat op zich geen gerubriceerde informatie is, tenzij het als zodanig wordt gemarkeerd;
 - d) wordt het document gedateerd;
 - e) worden documenten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger op elke bladzijde van een exemplaarnummer voorzien, indien zij in meerdere exemplaren moeten worden verspreid.
17. Als het niet mogelijk is punt 16 toe te passen op gerubriceerde EU-informatie, worden andere passende maatregelen genomen overeenkomstig de krachtens dit besluit op te stellen beveiligingsrichtsnoeren.

Verlagen van de rubricering en derubricering van gerubriceerde EU-informatie

18. Bij het genereren geeft de opsteller waar mogelijk, en in het bijzonder voor als RESTREINT UE/EU RESTRICTED gerubriceerde informatie, aan of de gerubriceerde EU-informatie op een bepaalde datum of na een bepaalde gebeurtenis lager gerubriceerd of gederubriceerd kan worden.
19. De EDEO herbekijkt regelmatig de gerubriceerde EU-informatie waarover hij beschikt om na te gaan of de rubriceringsgraad nog steeds van toepassing is. De EDEO stelt een regeling in om de rubriceringsgraad van geregistreerde gerubriceerde EU-informatie waarvan de EDEO de opsteller is, ten minste iedere vijf jaar te herbekijken. Deze controle is niet nodig wanneer de opsteller bij het genereren van de informatie heeft aangegeven dat deze automatisch lager gerubriceerd of gederubriceerd moet worden en de informatie dienovereenkomstig gemarkeerd is.

III. REGISTRATIE VAN GERUBRICEERDE EU-INFORMATIE VOOR BEVEILIGINGSDOELEINDEN

20. Op het hoofdkantoor van de EDEO wordt een centraal register ingesteld. Voor iedere organisatorische entiteit binnen de EDEO waar gerubriceerde EU-informatie wordt verwerkt, wordt een aan het centrale register ondergeschikt verantwoordelijk register aangewezen, teneinde te waarborgen dat gerubriceerde EU-informatie overeenkomstig dit besluit wordt verwerkt. De registers worden ingericht als beveiligde zones zoals omschreven in bijlage A.

Elke delegatie van de Unie stelt haar eigen register voor gerubriceerde EU-informatie in.

De veiligheidsautoriteit van de EDEO wijst voor deze registers een hoofd registratie aan.

21. Voor de toepassing van dit besluit wordt onder registratie voor beveiligingsdoeleinden (hierna „registratie” genoemd) verstaan: de toepassing van procedures waarbij de levenscyclus van materiaal, met inbegrip van de verspreiding en de vernietiging ervan, wordt geregistreerd. In het geval van een communicatie- en informatiesysteem kunnen de registratieprocedures worden uitgevoerd door middel van processen binnen het communicatie- en informatiesysteem zelf.
22. Alle materiaal met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger wordt geregistreerd wanneer het bij een organisatorische entiteit, waaronder delegaties van de Unie, aankomt of deze entiteit verlaat. Informatie met rubricering TRÈS SECRET UE/EU TOP SECRET wordt in speciaal daarvoor bestemde registers geregistreerd.
23. Het centrale register op het hoofdkantoor van de EDEO is het belangrijkste doorgangspunt voor de uitwisseling van gerubriceerde informatie met derde staten en internationale organisaties. In het centrale register wordt van elke uitwisseling een aantekening gemaakt.
24. Overeenkomstig artikel 14 van dit besluit stelt de hoge vertegenwoordiger beveiligingsrichtsnoeren inzake de registratie van gerubriceerde EU-informatie voor beveiligingsdoeleinden vast.

Registers voor TRÈS SECRET UE/EU TOP SECRET

25. Het centrale register op het hoofdkantoor van de EDEO wordt aangewezen als de centrale instantie voor het ontvangen en verzenden van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET. In voorkomend geval kunnen subregisters worden aangewezen voor de verwerking van dergelijke informatie voor registratiedoeleinden.
26. Deze subregisters mogen geen TRÈS SECRET UE/EU TOP SECRET-documenten rechtstreeks overdragen aan andere subregisters van hetzelfde centrale TRÈS SECRET UE/EU TOP SECRET-register, noch deze naar buiten toe overdragen, zonder uitdrukkelijke schriftelijke toestemming van het centrale register.

IV. KOPIËREN EN VERTALEN VAN GERUBRICEERDE EU-DOCUMENTEN

27. Documenten met rubricering TRÈS SECRET UE/EU TOP SECRET mogen niet zonder voorafgaande schriftelijke toestemming van de opsteller worden gekopieerd of vertaald.
28. Indien de opsteller van documenten met rubricering SECRET UE/EU SECRET of lager geen waarschuwingsmarkeringen met betrekking tot het kopiëren of vertalen heeft aangebracht, mogen deze documenten op instructie van de houder worden gekopieerd of vertaald.
29. De beveiligingsmaatregelen die voor het originele document gelden, zijn ook van toepassing op kopieën en vertalingen ervan. Kopieën van documenten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en hoger mogen uitsluitend worden vervaardigd door het betrokken register of subregister, met gebruikmaking van een beveiligd kopieerapparaat. De kopieën moeten worden geregistreerd.

V. VERVOER VAN GERUBRICEERDE EU-INFORMATIE

30. Voor het vervoer van gerubriceerde EU-informatie gelden de beschermende maatregelen van de punten 32 tot en met 42. Wanneer gerubriceerde EU-informatie op elektronische dragers wordt vervoerd, kunnen de onderstaande beschermende maatregelen onverminderd bijlage A, artikel 7, lid 4, worden aangevuld met passende door de veiligheidsautoriteit van de EDEO voorgeschreven technische tegenmaatregelen om het risico op verlies of compromittering zo klein mogelijk te maken.
31. De veiligheidsautoriteit van de EDEO geeft overeenkomstig dit besluit instructies over het vervoer van gerubriceerde EU-informatie.

Binnen een gebouw of op zichzelf staande groep van gebouwen

32. Gerubriceerde EU-informatie die binnen een gebouw of een op zichzelf staande groep van gebouwen wordt vervoerd, wordt afgedekt om te voorkomen dat de inhoud ervan zichtbaar is.
33. Binnen een gebouw of een op zichzelf staande groep van gebouwen wordt informatie met rubricering TRÈS SECRET UE/EU TOP SECRET vervoerd door personen met een passende veiligheidsmachtiging, in een beveiligde enveloppe met daarop alleen de naam van de geadresseerde.

Binnen de Europese Unie

34. Gerubriceerde EU-informatie die tussen gebouwen en locaties binnen de Europese Unie wordt vervoerd, wordt zodanig verpakt dat zij wordt beschermd tegen ongeoorloofde openbaarmaking.

35. Het vervoer binnen de Europese Unie van informatie met een rubriceringsgraad tot SECRET UE/EU SECRET geschiedt op één van de volgende wijzen:
- a) per militaire koerier, overheidskoerier of diplomatieke koerier, naargelang van het geval;
 - b) in handbagage, op voorwaarde dat:
 - i) de drager de gerubriceerde EU-informatie niet uit handen geeft, tenzij deze wordt opgeslagen conform de voorschriften van bijlage A II;
 - ii) de gerubriceerde EU-informatie niet onderweg wordt geopend of in het openbaar gelezen;
 - iii) de persoon de juiste veiligheidsmachtiging heeft en geïnstrueerd is over zijn verantwoordelijkheden inzake de beveiliging;
 - iv) de persoon zo nodig een koerierspas krijgt;
 - c) postdiensten of commerciële koeriersdiensten, op voorwaarde dat:
 - i) deze diensten door de desbetreffende nationale veiligheidsautoriteit zijn goedgekeurd overeenkomstig de nationale wet- en regelgeving;
 - ii) deze diensten adequate beschermingsmaatregelen toepassen overeenkomstig de minimumvoorschriften die worden vastgelegd in de krachtens artikel 21, lid 1, van dit besluit op te stellen beveiligingsrichtsnoeren.
- Bij vervoer van een lidstaat naar een andere wordt het bepaalde onder c) beperkt tot informatie tot en met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL.
36. Materiaal met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET (bijvoorbeeld apparaten of machines) dat niet kan worden vervoerd met de in punt 34 bedoelde middelen, wordt overeenkomstig bijlage A V als vracht vervoerd door commerciële vervoersondernemingen.
37. Het vervoer van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET tussen gebouwen of locaties binnen de Europese Unie geschiedt per militaire koerier, overheidskoerier of diplomatieke koerier, naargelang van het geval.

Vanuit de Europese Unie naar het grondgebied van een derde staat, of tussen EU-entiteiten binnen derde staten

38. Gerubriceerde EU-informatie die vanuit de Europese Unie naar het grondgebied van een derde staat of tussen EU-entiteiten binnen derde staten wordt vervoerd, wordt zodanig verpakt dat zij is beschermd tegen ongeoorloofde openbaarmaking.
39. Het vervoer van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET vanuit de Europese Unie naar het grondgebied van een derde staat en het vervoer van gerubriceerde EU-informatie tot aan het niveau SECRET UE/EU SECRET tussen EU-entiteiten binnen derde staten geschiedt op één van de volgende wijzen:
- a) per militaire of diplomatieke koerier;
 - b) in handbagage, op voorwaarde dat:
 - i) het pakket een officieel zegel draagt of zodanig is verpakt dat duidelijk is dat het om een officiële zending gaat die niet aan een douane- of veiligheidscontrole dient te worden onderworpen;
 - ii) de persoon een koerierspas bij zich heeft die het pakket identificeert en hem machtigt het te vervoeren;
 - iii) de drager de gerubriceerde EU-informatie niet uit handen geeft, tenzij deze wordt opgeslagen conform de voorschriften van bijlage A II;
 - iv) de gerubriceerde EU-informatie niet onderweg wordt geopend of in het openbaar gelezen, en
 - v) de persoon de juiste veiligheidsmachtiging heeft en geïnstrueerd is over zijn verantwoordelijkheden inzake de beveiliging.
40. Het vervoer van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET die door de Europese Unie wordt vrijgegeven aan een derde staat of een internationale organisatie, moet in overeenstemming zijn met de desbetreffende bepalingen van een informatiebeveiligingsovereenkomst of een administratieve regeling als bedoeld in bijlage A, artikel 10, lid 2.
41. Informatie met rubricering RESTREINT UE/EU RESTRICTED mag ook vanuit de EU naar het grondgebied van een derde staat door postdiensten of commerciële koeriersdiensten worden vervoerd.

42. Het vervoer van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET vanuit de Europese Unie naar het grondgebied van een derde staat of tussen EU-entiteiten binnen derde staten geschiedt per militaire of diplomatieke koerier.

VI. Vernietiging van gerubriceerde EU-informatie

43. Gerubriceerde EU-documenten die niet langer nodig zijn, mogen worden vernietigd onverminderd de geldende voorschriften inzake archivering.
44. Documenten die volgens bijlage A, artikel 7, lid 2, moeten worden geregistreerd, worden door het verantwoordelijke register vernietigd op instructie van de houder of een bevoegde autoriteit. De logboeken en andere informatie betreffende de registratie worden dienovereenkomstig bijgewerkt.
45. De vernietiging van documenten met rubricering SECRET UE/EU SECRET of TRÈS SECRET UE/EU TOP SECRET vindt plaats in het bijzijn van een getuige die gemachtigd is voor ten minste de rubriceringsgraad van het document dat wordt vernietigd.
46. Zowel de registrator als de getuige, als de aanwezigheid van deze laatste vereist is, ondertekenen een vernietigingscertificaat, dat in het register wordt bewaard. In het register worden vernietigingscertificaten van documenten met rubricering TRÈS SECRET UE/EU TOP SECRET gedurende ten minste tien jaar en van documenten met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL en SECRET UE/EU SECRET gedurende ten minste vijf jaar bewaard.
47. Om te voorkomen dat gerubriceerde documenten geheel of gedeeltelijk worden gereconstrueerd worden deze documenten, ook die met rubricering RESTREINT UE/EU RESTRICTED, vernietigd volgens methoden die voldoen aan de desbetreffende EU-normen of gelijkwaardige normen, of methoden die door de lidstaten zijn goedgekeurd volgens nationale technische normen.
48. De vernietiging van voor gerubriceerde EU-informatie gebruikte digitale opslagmedia geschiedt overeenkomstig door de veiligheidsautoriteit van de EDEO goedgekeurde procedures.

VII. Veiligheidsinspecties

Veiligheidsinspecties van de EDEO

49. Overeenkomstig artikel 16 van dit besluit omvatten de veiligheidsinspecties van de EDEO:
- a) algemene veiligheidsinspecties, die tot doel hebben het algemene beveiligingsniveau van het hoofdkantoor van de EDEO, de delegaties van de Unie en alle ondergeschikte of verwante locaties te beoordelen, en met name de doeltreffendheid van de veiligheidsmaatregelen die ter bescherming van de veiligheidsbelangen van de EDEO zijn getroffen;
 - b) veiligheidsinspecties voor gerubriceerde EU-informatie, die tot doel hebben de doeltreffendheid te beoordelen van de maatregelen die ter bescherming van gerubriceerde EU-informatie in het hoofdkantoor van de EDEO en de delegaties van de Unie zijn getroffen, doorgaans met het oog op homologatie.

Deze inspecties moeten met name worden verricht om onder meer:

- i) te waarborgen dat de bij dit besluit vastgestelde verplichte minimumnormen voor de bescherming van gerubriceerde EU-informatie worden nageleefd;
- ii) het belang van beveiliging en doeltreffende risicobeheersing binnen de geïnspecteerde entiteiten te benadrukken;
- iii) tegenmaatregelen aan te bevelen om de specifieke gevolgen van de aantasting van de vertrouwelijkheid, integriteit of beschikbaarheid van gerubriceerde informatie te beperken, en
- iv) de lopende opleidings- en bewustmakingsprogramma's die door de veiligheidsautoriteiten met betrekking tot beveiliging worden uitgevoerd, te versterken.

Uitvoering van en rapportage over veiligheidsinspecties van de EDEO

50. De veiligheidsinspecties van de EDEO worden uitgevoerd door een inspectieteam van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, en, waar nodig, met steun van beveiligingsexperts van andere EU-instellingen of lidstaten.

Het inspectieteam heeft toegang tot iedere locatie waar gerubriceerde EU-informatie wordt verwerkt, en met name de registers en de plaatsen waar communicatie- en informatiesystemen aanwezig zijn.

51. De veiligheidsinspecties van de EDEO in de delegaties van de Unie kunnen zo nodig worden uitgevoerd met steun van de beveiligingsfunctionarissen van de ambassades van de lidstaten in derde landen.
52. Voor het einde van ieder kalenderjaar stelt de veiligheidsautoriteit van de EDEO een veiligheidsinspectieprogramma voor de EDEO voor het volgende jaar vast.
53. Waar nodig kan de veiligheidsautoriteit van de EDEO veiligheidsinspecties houden die niet in het hierboven bedoelde programma zijn opgenomen.
54. Na afloop van de veiligheidsinspectie worden de belangrijkste conclusies en aanbevelingen aan de geïnspecteerde entiteit voorgelegd. Vervolgens stelt het inspectieteam een inspectieverslag op. Indien corrigerende maatregelen en aanbevelingen zijn voorgesteld, moet het verslag voldoende nadere informatie bevatten ter ondersteuning van de getrokken conclusies. Het verslag wordt aan de veiligheidsautoriteit van de EDEO en aan het hoofd van de geïnspecteerde entiteit toegezonden.

Onder de verantwoordelijkheid van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, wordt op gezette tijden een verslag opgesteld met, voor een specifieke periode, de lessen die uit de inspecties zijn getrokken en door het Beveiligingscomité van de EDEO zijn bestudeerd.

Uitvoering van en rapportage over veiligheidsinspecties van EU-organen en -instanties die uit hoofde van titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie (VEU) zijn opgericht

55. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, kan waar nodig deskundigen aanwijzen om deel te nemen aan gezamenlijke EU-inspectieteams die inspecties uitvoeren in EU-organen en -instanties die uit hoofde van titel V, hoofdstuk 2, VEU zijn opgericht.

Checklist voor veiligheidsinspecties van de EDEO

56. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, stelt een checklist voor beveiligingsinspecties op, en werkt deze zo nodig bij, met de punten die tijdens een veiligheidsinspectie van de EDEO moeten worden geverifieerd. Deze checklist wordt aan het Beveiligingscomité van de EDEO toegezonden.
57. De informatie ter uitvoering van de checklist wordt, in het bijzonder tijdens de inspectie, verkregen bij de voor het beveiligingsbeheer bevoegde functionarissen van de entiteit die wordt geïnspecteerd. Zodra de checklist met de gedetailleerde antwoorden is aangevuld, wordt hij in overleg met de geïnspecteerde entiteit gerubriceerd. De checklist maakt geen deel uit van het inspectieverslag.

BIJLAGE A IV

BESCHERMING VAN IN COMMUNICATIE- EN INFORMATIESYSTEMEN VERWERKTE GERUBRICEERDE EU-INFORMATIE

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 8.
2. Onderstaande eigenschappen en concepten op het gebied van information assurance (hierna „IA” genoemd) zijn essentieel voor de beveiliging en de correcte werking van operaties met communicatie- en informatiesystemen.

Authenticiteit:	de garantie dat informatie echt en ongewijzigd is en van bonafide bronnen afkomstig is.
Beschikbaarheid:	de eigenschap dat informatie op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar is.
Vertrouwelijkheid:	de eigenschap dat informatie niet wordt vrijgegeven aan niet-gemachtigde personen, entiteiten of processen.
Integriteit:	de eigenschap dat de nauwkeurigheid en de volledigheid van de informatie en de functionele bestanddelen is gewaarborgd.
Onweerlegbaarheid:	de eigenschap dat bewezen kan worden dat een actie of gebeurtenis heeft plaatsgevonden, zodat deze actie of gebeurtenis niet vervolgens kan worden ontkend.

II. BEGINSELEN VAN IA

3. De onderstaande bepalingen vormen de basis voor de beveiliging van alle communicatie- en informatiesystemen die voor het verwerken van gerubriceerde EU-informatie worden gebruikt. In de IA-beveiligingsrichtsnoeren moeten uitgebreide voorschriften voor de uitvoering van deze bepalingen worden vastgelegd.

Beheersing van beveiligingsrisico's

4. Beheersing van veiligheidsrisico's is een integrerend onderdeel van het definiëren, ontwikkelen, exploiteren en onderhouden van een communicatie- en informatiesysteem. Risicobeheersing (beoordeling, behandeling, aanvaarding en communicatie) verloopt als een zich herhalend proces dat gezamenlijk wordt uitgevoerd door vertegenwoordigers van de eigenaren van het systeem, projectautoriteiten, exploitanten en veiligheidsgoedkeuringsinstanties, waarbij gebruik wordt gemaakt van een beproefde, transparante en volledig begrijpelijke risicobeoordelingsprocedure. De reikwijdte van het communicatie- en informatiesysteem en de functionele bestanddelen ervan wordt aan het begin van het risicobeheersingsproces duidelijk afgebakend.
5. De bevoegde autoriteiten van de EDEO herbekijken de mogelijke dreigingen voor communicatie- en informatiesystemen en zorgen voor bijgewerkte en nauwkeurige dreigingsbeoordelingen die weergeven hoe de operationele omgeving van dat moment is. Zij werken voortdurend hun kennis inzake kwetsbaarheden bij en herzien op gezette tijden de kwetsbaarheidsbeoordeling, met het oog op aanpassing aan de veranderende informatietechnologie(IT)-omgeving.
6. De beheersing van veiligheidsrisico's is gericht op de toepassing van een geheel van beveiligingsmaatregelen dat een bevredigend evenwicht oplevert tussen de gebruikerseisen en het residuele veiligheidsrisico.
7. De door de bevoegde veiligheidshomologatieautoriteit vastgestelde specifieke eisen, reikwijdte en gedetailleerdheid die voor de homologatie van een communicatie- en informatiesysteem vereist zijn, stemmen overeen met het ingeschatte risico, rekening houdend met alle relevante factoren, waaronder de rubriceringsgraad van de in het communicatie- en informatiesysteem verwerkte gerubriceerde EU-informatie. Homologatie houdt mede een formele verklaring betreffende het residuele risico in en aanvaarding van dat residuele risico door een verantwoordelijke autoriteit.

Beveiliging gedurende de levenscyclus van het communicatie- en informatiesysteem

8. Beveiliging is gedurende de gehele levenscyclus van het communicatie- en informatiesysteem — vanaf de ingebruikname tot de buitengebruikstelling — een vereiste.

9. De rol en interactie van iedere bij een communicatie- en informatiesysteem betrokken partij in verband met de beveiliging ervan wordt voor iedere fase van de levenscyclus vastgesteld.
10. Alle communicatie- en informatiesystemen, met inbegrip van de maatregelen voor de technische en niet-technische beveiliging ervan, worden tijdens de homologatieprocedure aan beveiligingstests onderworpen om ervoor te zorgen dat het passende niveau van IA wordt bereikt en om na te gaan of zij correct zijn geïmplementeerd, geïntegreerd en geconfigureerd.
11. Beveiligingsbeoordelingen, inspecties en evaluaties worden verricht op gezette tijden tijdens de werking en het onderhoud van een communicatie- en informatiesystemen en tevens wanneer zich uitzonderlijke omstandigheden voordoen.
12. De beveiligingsdocumentatie voor een communicatie- en informatiesysteem evolueert gedurende de levenscyclus van dat communicatie- en informatiesysteem als een integrerend onderdeel van het proces van wijzigings- en configuratiebeheer.

Beste praktijken

13. De EDEO ontwikkelt samen met het secretariaat-generaal van de Raad, de Commissie en de lidstaten beste praktijken voor de bescherming van in communicatie- en informatiesystemen verwerkte gerubriceerde EU-informatie. In de richtsnoeren voor beste praktijken worden technische, fysieke, organisatorische en procedurele beveiligingsmaatregelen voor communicatie- en informatiesystemen beschreven waarvan is aangetoond dat zij doeltreffend zijn voor het bestrijden van dreigingen en kwetsbaarheden.
14. Bij de bescherming van in communicatie- en informatiesystemen verwerkte gerubriceerde EU-informatie wordt gebruikgemaakt van de lessen die door de bij IA betrokken entiteiten, zowel binnen als buiten de EU, zijn getrokken.
15. De verspreiding en de daaropvolgende toepassing van de beste praktijken dragen bij tot het bereiken van eenzelfde niveau van IA voor de diverse communicatie- en informatiesystemen van de EDEO waarin gerubriceerde EU-informatie wordt verwerkt.

Defence in depth

16. Om het risico voor communicatie- en informatiesystemen tot een minimum te beperken, wordt een aantal technische en niet-technische beveiligingsmaatregelen genomen, in de vorm van meerdere verdedigingslagen. Deze lagen omvatten:
 - a) *afschrikking*: beveiligingsmaatregelen waarmee vijandelijke plannen om het communicatie- en informatiesysteem aan te vallen, worden ontmoedigd;
 - b) *preventie*: beveiligingsmaatregelen waarmee een aanval op het communicatie- en informatiesysteem wordt verhinderd of tegengehouden;
 - c) *detectie*: beveiligingsmaatregelen waarmee wordt ontdekt dat het communicatie- en informatiesysteem wordt aangevallen;
 - d) *veerkracht*: beveiligingsmaatregelen waarmee het effect van een aanval tot een zo klein mogelijke hoeveelheid informatie of onderdelen van communicatie- en informatiesysteem wordt beperkt en verdere schade wordt voorkomen, en
 - e) *herstel*: beveiligingsmaatregelen waarmee weer een veilige situatie voor het communicatie- en informatiesysteem tot stand wordt gebracht.

Aan de hand van een risicobeoordeling wordt de mate van striktheid en toepasselijkheid van die beveiligingsmaatregelen bepaald.

17. De bevoegde autoriteiten van de EDEO zorgen ervoor dat zij in staat zijn te reageren op incidenten die wellicht de organisatorische en nationale grenzen overschrijden en dat zij de respons kunnen coördineren en informatie uitwisselen over deze incidenten en de ermee verband houdende risico's (responscapaciteit voor computercalamiteiten).

Beginsel van minimale gegevensverwerking en het minste voorrecht

18. Om onnodige risico's te vermijden worden uitsluitend de functies, apparaten en diensten geactiveerd die essentieel zijn voor het vervullen van de operationele eisen.

19. Gebruikers van een communicatie- en informatiesysteem en geautomatiseerde processen krijgen alleen de toegang, voorrechten of machtigingen die zij nodig hebben voor het uitvoeren van hun taken, zodat schade door ongelukken, vergissingen of ongeoorloofd gebruik van middelen van communicatie- en informatiesystemen beperkt blijft.
20. De door een communicatie- en informatiesysteem uitgevoerde registratieprocedures worden indien nodig geverifieerd als onderdeel van de homologatieprocedure.

Bewustwording van information assurance

21. De eerste verdedigingslaag voor de beveiliging van communicatie- en informatiesystemen bestaat uit bewustwording van de risico's en bekendheid met de beschikbare beveiligingsmaatregelen. Met name moeten alle personeelsleden die betrokken zijn bij de levenscyclus van communicatie- en informatiesystemen, met inbegrip van de gebruikers, inzien dat:
 - a) beveiligingsfouten ernstige schade kunnen berokkenen aan de communicatie- en informatiesystemen en de gehele organisatie;
 - b) interconnectiviteit en onderlinge afhankelijkheid kunnen leiden tot schade voor anderen, en
 - c) zij individuele verantwoordelijkheid en aansprakelijkheid dragen voor de beveiliging van communicatie- en informatiesystemen overeenkomstig hun functie binnen de systemen en processen.
22. Alle betrokken personeelsleden, onder meer het hogere management en de gebruikers van communicatie- en informatiesystemen, moeten verplicht een IA-opleiding en -bewustwordingstraining volgen, zodat goed wordt begrepen waar de verantwoordelijkheden inzake beveiliging liggen.

Evaluatie en goedkeuring van IT-beveiligingsproducten

23. De vereiste graad van vertrouwen in de beveiligingsmaatregelen, gedefinieerd als een niveau van IA, wordt bepaald aan de hand van de resultaten van het risicobeheersingsproces en het beveiligingsbeleid en de beveiligingsrichtsnoeren in kwestie.
24. Het niveau van IA wordt geverifieerd door middel van internationaal erkende of nationaal goedgekeurde processen en methoden. Deze omvatten in de eerste plaats evaluatie, controles en audits.
25. Encryptieproducten voor de bescherming van gerubriceerde EU-informatie worden geëvalueerd en goedgekeurd door de autoriteit voor de goedkeuring van encryptieproducten (hierna „CAA” genoemd) van een lidstaat.
26. Voordat encryptieproducten worden aanbevolen voor goedkeuring door de CAA van de EDEO overeenkomstig artikel 8, lid 5, moeten zij zijn onderworpen aan een succesvolle onafhankelijke evaluatie door een naar behoren gekwalificeerde instantie (hierna „AQUA” genoemd) van een lidstaat die niet betrokken is bij het ontwerp of de vervaardiging van de apparatuur. Hoe uitvoerig een en ander tijdens deze onafhankelijke evaluatie moet worden bekeken, hangt af van de beoogde maximale rubriceringsgraad van de gerubriceerde EU-informatie die door deze producten moet worden beschermd.
27. Wanneer zulks om specifieke operationele redenen gerechtvaardigd is, kan de CAA van de EDEO op aanbeveling van het Beveiligingscomité afwijken van de vereisten van de punten 25 en 26 en een tijdelijke goedkeuring voor een specifieke periode verlenen overeenkomstig artikel 8, lid 5, van dit besluit.
28. Een AQUA is een CAA van een lidstaat die op basis van door de Raad vastgestelde criteria is geaccrediteerd voor het uitvoeren van de onafhankelijke evaluatie van encryptieproducten voor de bescherming van gerubriceerde EU-informatie.
29. De hoge vertegenwoordiger stelt een beveiligingsbeleid vast inzake de kwalificatie en goedkeuring van IT-beveiligingsproducten die geen encryptieproducten zijn.

Overdracht binnen beveiligde zones

30. Niettegenstaande het bepaalde in dit besluit kan, wanneer de overdracht van gerubriceerde EU-informatie beperkt is tot beveiligde zones, op basis van het resultaat van een risicobeheersingsproces en behoudens goedkeuring van de veiligheidshomologatieautoriteit, gebruik worden gemaakt van onversleutelde verspreiding of van versleuteling op een lager niveau.

Beveiligde interconnectie van communicatie- en informatiesystemen

31. In dit besluit wordt onder een interconnectie verstaan: een rechtstreekse koppeling van twee of meer IT-systemen, met als doel het gezamenlijk gebruik van informatie en andere bronnen van informatie (bijvoorbeeld communicatie), in één of meer richtingen.
32. Een communicatie- en informatiesysteem dient ieder gekoppeld IT-systeem als niet-vertrouwd te beschouwen en beschermende maatregelen te activeren om de uitwisseling van gerubriceerde informatie te controleren.
33. Voor alle interconnecties van communicatie- en informatiesystemen met een ander IT-systeem moet worden voldaan aan de volgende basisvereisten:
 - a) de zakelijke of operationele vereisten voor dergelijke interconnecties worden door de bevoegde autoriteiten vastgelegd en goedgekeurd;
 - b) de interconnecties worden aan een procedure inzake risicobeheersing en homologatie onderworpen en moeten worden goedgekeurd door de bevoegde veiligheidshomologatieautoriteiten, en
 - c) de perimeters van alle communicatie- en informatiesystemen worden opgezet met voorzieningen om de grenzen te beschermen (Boundary Protection Services, hierna „BPS” genoemd).
34. Er mag geen interconnectie tot stand worden gebracht tussen een gehomologeerd communicatie- en informatiesysteem en een onbeschermd of openbaar netwerk, tenzij voor dat doel in het communicatie- en informatiesysteem goedgekeurde BPS zijn opgezet om de grenzen te beschermen tussen het communicatie- en informatiesysteem en het onbeschermd of openbare netwerk. De beveiligingsmaatregelen voor dergelijke interconnecties worden getoetst door de bevoegde IA-autoriteit en goedgekeurd door de bevoegde veiligheidshomologatieautoriteit.

Wanneer het onbeschermd of openbare netwerk alleen als drager wordt gebruikt en de informatie versleuteld is met een overeenkomstig artikel 8, lid 5, van dit besluit goedgekeurd encryptieproduct, wordt een dergelijke koppeling niet gezien als een interconnectie.

35. Rechtstreekse interconnectie of interconnectie in cascade van een communicatie- en informatiesysteem dat gehomologeerd is voor de verwerking van informatie met rubricering TRÈS SECRET UE/EU TOP SECRET, en een onbeschermd of openbaar netwerk, is verboden.

Digitale opslagmedia

36. Digitale opslagmedia worden vernietigd volgens procedures die de veiligheidsautoriteit van de EDEO heeft goedgekeurd.
37. Digitale opslagmedia worden hergebruikt, lager gerubriceerd of gederubriceerd conform een overeenkomstig artikel 8, lid 2, van dit besluit vast te stellen beveiligingsrichtsnoeren.

Noodgevallen

38. Niettegenstaande het bepaalde in dit besluit mogen in noodgevallen, zoals dreigende of uitgebroken crises, conflicten, oorlogssituaties of in uitzonderlijke operationele omstandigheden, gedurende een beperkte periode de hieronder beschreven specifieke procedures worden toegepast.
39. Gerubriceerde EU-informatie mag met toestemming van de bevoegde autoriteit door middel van voor een lagere rubriceringsgraad goedgekeurde encryptieproducten of zonder versleuteling worden overgedragen, indien elke vertraging schade zou veroorzaken die duidelijk zwaarder weegt dan de schade ten gevolge van de verspreiding van het gerubriceerde materiaal en indien:
 - a) de zender en de ontvanger niet over de vereiste encryptieapparatuur beschikken of helemaal geen encryptieapparatuur hebben, en
 - b) het gerubriceerde materiaal niet op tijd met andere middelen kan worden verstuurd.
40. Gerubriceerde informatie die in de in punt 39 bedoelde omstandigheden wordt overgedragen, mag geen tekenen of aanwijzingen dragen waardoor zij kan worden onderscheiden van ongerubriceerde informatie of informatie die beschermd kan worden door middel van een beschikbaar encryptieproduct. De ontvangers worden onverwijld langs andere wegen op de hoogte gebracht van de rubriceringsgraad.

41. Indien punt 39 wordt toegepast, wordt nadien verslag uitgebracht aan het directoraat van de EDEO dat verantwoordelijk is voor beveiliging en via dat directoraat aan het Beveiligingscomité van de EDEO. In het verslag worden in ieder geval de verzender, de ontvanger en de opsteller van alle gerubriceerde EU-informatie vermeld.

III. FUNCTIES EN AUTORITEITEN OP HET GEBIED VAN INFORMATION ASSURANCE

42. Bij de EDEO worden onderstaande functies op het gebied van IA ingesteld. Deze functies vereisen geen afzonderlijke organisatorische entiteiten. Zij hebben afzonderlijke mandaten. Deze functies en de ermee samengaande verantwoordelijkheden kunnen echter in één organisatorische entiteit worden ondergebracht of geïntegreerd dan wel in meerdere organisatorische entiteiten worden gesplitst, als maar wordt vermeden dat belangen of taken botsen.

IA-autoriteit (hierna „IAA” genoemd)

43. De IAA is verantwoordelijk voor:
- a) het ontwikkelen van IA-beveiligingsrichtsnoeren en het toezien op de doeltreffendheid en relevantie daarvan;
 - b) het beschermen en beheren van technische informatie over encryptieproducten;
 - c) het garanderen dat IA-maatregelen die voor de bescherming van gerubriceerde EU-informatie zijn geselecteerd, voldoen aan de richtsnoeren inzake de geschiktheid en selectie van die maatregelen;
 - d) het garanderen dat encryptieproducten worden geselecteerd overeenkomstig de richtsnoeren inzake de geschiktheid en selectie ervan;
 - e) het coördineren van opleiding en voorlichting inzake IA;
 - f) het overleggen over de IA-beveiligingsrichtsnoeren met de systeemaanbieder, de beveiligingsmedewerkers en de vertegenwoordigers van gebruikers, en
 - g) het garanderen dat er in het IA-expertisedeelgebied van het Beveiligingscomité van de EDEO passende deskundigheid beschikbaar is.

TEMPEST-autoriteit

44. De TEMPEST-autoriteit is ervoor verantwoordelijk dat communicatie- en informatiesystemen in overeenstemming zijn met het TEMPEST-beleid en de TEMPEST-richtsnoeren. Zij keurt TEMPEST-tegenmaatregelen voor installaties en producten goed die bestemd zijn voor de bescherming van gerubriceerde EU-informatie tot een bepaalde rubriceringsgraad in haar operationele omgeving.

Autoriteit voor de goedkeuring van encryptieproducten (hierna „CAA” genoemd)

45. De CAA is ervoor verantwoordelijk dat encryptieproducten voldoen aan de geldende cryptografierichtsnoeren. De CAA verleent aan een encryptieproduct goedkeuring voor de bescherming van gerubriceerde EU-informatie tot een bepaalde rubriceringsgraad in haar operationele omgeving.

Autoriteit voor de distributie van encryptieproducten (hierna „CDA” genoemd)

46. De CDA is verantwoordelijk voor:
- a) het beheer van en de verantwoording voor encryptiemateriaal van de Europese Unie;
 - b) de naleving van passende procedures en de instelling van kanalen voor verslaglegging over, en veilige verwerking, opslag en verspreiding van al het encryptiemateriaal van de Europese Unie, en
 - c) de overdracht van encryptiemateriaal van de Europese Unie aan of van personen of diensten die er gebruik van maken.

Veiligheidshomologatieautoriteit (hierna „SAA” genoemd)

47. De SAA voor ieder systeem is verantwoordelijk voor:
- a) het garanderen dat communicatie- en informatiesystemen voldoen aan de toepasselijke beveiligingsrichtsnoeren, door het afgeven van een goedkeuringsverklaring voor communicatie- en informatiesystemen voor de verwerking van gerubriceerde EU-informatie tot een bepaalde rubriceringsgraad in haar operationele omgeving, met de voorwaarden voor de homologatie, en de criteria volgens welke nieuwe goedkeuring nodig is;

- b) het instellen van een procedure voor veiligheidshomologatie, overeenkomstig de desbetreffende richtsnoeren, met duidelijke goedkeuringsvoorwaarden voor communicatie- en informatiesystemen die onder haar gezag staan;
 - c) het vaststellen van een strategie voor veiligheidshomologatie waarin de mate van gedetailleerdheid voor de homologatie wordt aangegeven, afhankelijk van het vereiste IA-niveau;
 - d) het bestuderen en goedkeuren van beveiligingsdocumentatie, waaronder verklaringen over risicobeheersing en residuele risico's, systeemspecifieke verklaringen van beveiligingseisen, documentatie voor de verificatie van de beveiligingsimplementatie en operationele beveiligingsprocedures, en het garanderen dat die documentatie in overeenstemming is met de beveiligingsvoorschriften en -richtsnoeren van de EDEO;
 - e) het controleren van de implementatie van beveiligingsmaatregelen met betrekking tot de communicatie- en informatiesystemen, namelijk door het uitvoeren of ondersteunen van beveiligingsbeoordelingen, -inspecties en -toetsingen;
 - f) het vaststellen van beveiligingseisen (bijvoorbeeld inzake veiligheidsmachtigingen) voor gevoelige posten in verband met communicatie- en informatiesystemen;
 - g) het onderschrijven van de selectie van goedgekeurde encryptie- en TEMPEST-producten die worden gebruikt om een communicatie- en informatiesysteem te beveiligen;
 - h) het goedkeuren, of indien nodig, het deelnemen aan de gezamenlijke goedkeuring van de interconnectie van een communicatie- en informatiesysteem met andere communicatie- en informatiesystemen, en
 - i) het overleggen met de systeemaanbieder, de beveiligingsmedewerkers en vertegenwoordigers van de gebruikers over veiligheidsrisicobeheersing, in het bijzonder het residuele risico en de voorwaarden voor de goedkeuringsverklaring.
48. De SAA van de EDEO is verantwoordelijk voor de homologatie van alle communicatie- en informatiesystemen die binnen de EDEO worden gebruikt.

Veiligheidshomologatieorgaan (hierna „SAB” genoemd)

49. Een gemeenschappelijk veiligheidshomologatieorgaan is verantwoordelijk voor de homologatie van communicatie- en informatiesystemen die onder de bevoegdheid vallen van de SAA van de EDEO en de SAA's van de lidstaten. Het bestaat uit vertegenwoordigers van de SAA van iedere lidstaat; de vergaderingen worden bijgewoond door een vertegenwoordiger van de SAA van het secretariaat-generaal van de Raad en de Commissie. Andere entiteiten met een aansluiting op een communicatie- en informatiesysteem wordt verzocht vergaderingen bij te wonen waarin dat systeem wordt besproken.

Het SAB wordt voorgezeten door een vertegenwoordiger van de SAA van de EDEO. Het neemt besluiten met eenparigheid van stemmen van de SAA-vertegenwoordigers van instellingen, lidstaten en andere entiteiten met aansluitingen op de communicatie- en informatiesystemen. Het brengt periodiek verslag over zijn werkzaamheden uit aan het Beveiligingscomité van de EDEO en stelt dit in kennis van alle homologatieverklaringen.

Operationele autoriteit voor information assurance

50. De operationele IA-autoriteit voor ieder systeem is verantwoordelijk voor:
- a) het ontwikkelen van beveiligingsdocumentatie in overeenstemming met de beveiligingsrichtsnoeren, in het bijzonder de systeemspecifieke verklaring van beveiligingseisen en de verklaring inzake het residuele risico, de operationele beveiligingsprocedures en het encryptieplan dat deel uitmaakt van de homologatieprocedure voor communicatie- en informatiesystemen;
 - b) het deelnemen aan de selectie en het testen van systeemspecifieke maatregelen, apparatuur en software voor technische beveiliging, teneinde toezicht te houden op de implementatie ervan en ervoor te zorgen dat zij veilig worden geïnstalleerd, geconfigureerd en onderhouden overeenkomstig de beveiligingsdocumentatie;
 - c) het deelnemen aan de selectie van TEMPEST-beveiligingsmaatregelen en -apparatuur indien dat volgens de systeemspecifieke verklaring van beveiligingseisen nodig is, en ervoor zorgen dat zij veilig worden geïnstalleerd en onderhouden, in samenwerking met de TEMPEST-autoriteit;
 - d) het toezien op de uitvoering en toepassing van de operationele beveiligingsprocedures en, in voorkomend geval, het overdragen van operationele verantwoordelijkheden voor beveiliging aan de eigenaar van het systeem;

- e) het beheren en toepassen van encryptieproducten, het bewaren van versleutelde en gecontroleerde informatie en, indien nodig, het genereren van cryptografische variabelen;
 - f) het uitvoeren van evaluaties en tests van veiligheidsanalyses, in het bijzonder om de door de SAA verlangde risicoverslagen op te stellen;
 - g) het aanbieden van communicatie- en informatiesysteem-specifieke IA-opleidingen;
 - h) het implementeren en toepassen van communicatie- informatiesysteem-specifieke beveiligingsmaatregelen.
-

BIJLAGE A V

INDUSTRIËLE BEVEILIGING**I. INLEIDING**

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 9. De bijlage bevat algemene beveiligingsbepalingen die voor industriële of andere entiteiten gelden in precontractuele onderhandelingen en gedurende de levenscyclus van gerubriceerde opdrachten die de EDEO gunt.
2. De veiligheidsautoriteit van de EDEO stelt richtsnoeren inzake industriële beveiliging vast waarin in het bijzonder uitvoerige vereisten worden geformuleerd inzake veiligheidsmachtigingen voor vestigingen, memoranda over beveiligingsaspecten, bezoeken, en overdracht en vervoer van gerubriceerde EU-informatie.

II. BEVEILIGINGSELEMENTEN IN EEN GERUBRICEERDE OPDRACHT**Rubriceringsgids**

3. Alvorens een aanbesteding uit te schrijven of een gerubriceerde opdracht te gunnen, bepaalt de EDEO als aanbestedende instantie welke rubricering wordt gegeven aan informatie die aan inschrijvers en contractanten moet worden verstrekt, en welke rubricering wordt gegeven aan informatie die de contractant zal genereren. Voor dat doel stelt de EDEO een rubriceringsgids op die bij de uitvoering van de opdracht moet worden gebruikt.
4. Voor het bepalen van de rubricering van de diverse onderdelen van een gerubriceerde opdracht gelden onderstaande beginselen:
 - a) bij het opstellen van een rubriceringsgids houdt de EDEO rekening met alle relevante beveiligingsaspecten, zoals de rubricering die is gegeven aan verstrekte informatie waarvan het gebruik voor de opdracht is goedgekeurd door de opsteller van de informatie;
 - b) de algehele rubriceringsgraad van de opdracht mag niet lager zijn dan de hoogste rubricering van de onderdelen ervan, en
 - c) indien nodig neemt de EDEO contact op met de nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten van de lidstaten of enige andere bevoegde veiligheidsautoriteit, als zich wijzigingen voordoen met betrekking tot de rubricering van informatie die door of aan contractanten is verstrekt tijdens de uitvoering van een opdracht, en wanneer verdere wijzigingen in de rubriceringsgids worden aangebracht.

Memorandum over beveiligingsaspecten

5. De specifieke beveiligingseisen voor de opdracht worden beschreven in een memorandum over beveiligingsaspecten. Dit memorandum bevat in voorkomend geval de rubriceringsgids en maakt integraal deel uit van een gerubriceerde opdracht of opdracht in onderaanneming.
6. Het memorandum over beveiligingsaspecten bevat bepalingen die de contractant en/of de subcontractant verplichten zich te houden aan de minimumbeveiligingsnormen van dit besluit. Niet-naleving van deze minimumnormen kan voldoende grond zijn voor opzegging van de opdracht.

Programma-/projectbeveiligingsinstructies

7. Afhankelijk van het toepassingsgebied van programma's of projecten waarvoor toegang tot of verwerking of opslag van gerubriceerde EU-informatie nodig is, kan de aanbestedende instantie die het programma of het project zal beheren, specifieke programma-/projectbeveiligingsinstructies opstellen. De programma-/projectbeveiligingsinstructies moeten worden goedgekeurd door de nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten van de lidstaten of een andere bevoegde veiligheidsautoriteit die deelneemt aan het programma/project, en kunnen nadere beveiligingsvoorschriften bevatten.

III. VEILIGHEIDSMACHTIGINGEN VOOR VESTIGINGEN

8. Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, verzoekt de nationale veiligheidsautoriteit, de aangewezen veiligheidsautoriteit of een andere bevoegde instantie van de betrokken lidstaat een veiligheidsmachtiging voor een vestiging af te geven, die overeenkomstig de nationale wet- en regelgeving bevestigt dat een industriële of andere entiteit binnen haar vestigingen in staat is gerubriceerde EU-informatie te beschermen op het vereiste rubriceringsniveau (CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET). Voordat aan een contractant of subcontractant of een mogelijke contractant of subcontractant gerubriceerde EU-informatie mag worden verstrekt of toegang tot gerubriceerde EU-informatie mag worden verleend, dient aan de EDEO bewijs te worden verstrekt dat de veiligheidsmachtiging is afgegeven.
9. In voorkomend geval deelt de EDEO, als aanbestedende instantie, de betrokken nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit mee dat in de precontractuele fase of voor de uitvoering van de opdracht een veiligheidsmachtiging voor een vestiging vereist is. Een veiligheidsmachtiging voor een vestiging of een veiligheidsmachtiging voor een persoon is in de precontractuele fase vereist, wanneer gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET moet worden verstrekt in het stadium van de offertes.
10. De EDEO als aanbestedende instantie gunt geen gerubriceerde opdracht aan de geselecteerde inschrijver zonder van de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit van de lidstaat waar de contractant of subcontractant is geregistreerd, de bevestiging te hebben ontvangen dat er, indien zulks vereist is, een veiligheidsmachtiging voor een vestiging is afgegeven.
11. De EDEO als aanbestedende instantie verzoekt de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit die een veiligheidsmachtiging voor een vestiging heeft afgegeven, om op de hoogte te worden gesteld van wijzigingen die gevolgen hebben voor de veiligheidsmachtiging voor een vestiging. Bij onderaanneming wordt de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit op de hoogte gebracht.
12. Intrekking van een veiligheidsmachtiging voor een vestiging door de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit is voor de EDEO als aanbestedende instantie voldoende grond om een gerubriceerde opdracht te beëindigen of een inschrijver van mededinging uit te sluiten.

IV. VEILIGHEIDSMACHTIGINGEN VOOR HET PERSONEEL VAN CONTRACTANTEN

13. Alle voor contractanten werkende personeelsleden die toegang tot gerubriceerde EU-informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger moeten hebben, dienen een veiligheidsmachtiging van het vereiste niveau te hebben en een noodzaak tot kennisname te hebben voor die informatie. Hoewel een veiligheidsmachtiging niet nodig is voor de toegang tot gerubriceerde EU-informatie met rubricering RESTREINT UE/EU RESTRICTED, is de noodzaak tot kennisname wel vereist.
14. De aanvragen voor veiligheidsmachtigingen voor de personeelsleden van contractanten worden ingediend bij de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit die voor de entiteit bevoegd is.
15. De EDEO wijst contractanten die een onderdaan van een derde staat in dienst willen nemen op een post waarvoor toegang tot gerubriceerde EU-informatie vereist is, erop dat het de taak van de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit van de lidstaat waar de werkgever is gevestigd om te bepalen of de betrokkene toegang kan worden verleend tot dergelijke informatie, overeenkomstig dit besluit, en te bevestigen dat de opsteller van de informatie toestemming moet hebben gegeven voordat toegang kan worden verleend.

V. GERUBRICEERDE OPDRACHTEN EN ONDERAANNEMING

16. Wanneer in de precontractuele fase gerubriceerde EU-informatie wordt verstrekt aan een inschrijver, bevat de uitnodiging tot inschrijving een bepaling die de inschrijver die uiteindelijk geen offerte doet, of die niet wordt geselecteerd, verplicht alle gerubriceerde documenten binnen een bepaalde termijn terug te zenden.
17. Zodra een gerubriceerde opdracht of opdracht in onderaanneming is gegund, deelt de EDEO als aanbestedende instantie de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit van de contractant of subcontractant de beveiligingsbepalingen van de gerubriceerde opdracht mee.
18. Wanneer zulke opdrachten aflopen of worden beëindigd, deelt de EDEO als aanbestedende dienst (en/of, bij onderaanneming, de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit, naargelang van het geval) dit mee aan de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit van de lidstaat waar de contractant of subcontractant is geregistreerd.

19. Als algemene regel geldt dat de contractant of subcontractant alle gerubriceerde EU-informatie die hij in zijn bezit heeft, na voltooiing of beëindiging van de gerubriceerde opdracht of onderaanneming moet terugbezorgen aan de aanbestedende instantie.
20. In het memorandum over beveiligingsaspecten worden specifieke bepalingen opgenomen voor het verwijderen van gerubriceerde EU-informatie tijdens de uitvoering van een opdracht of bij de voltooiing of beëindiging ervan.
21. Wanneer de contractant of subcontractant gemachtigd is gerubriceerde EU-informatie te behouden na voltooiing of beëindiging van een opdracht, blijven de minimumnormen van dit besluit van toepassing en dient de vertrouwelijkheid van de gerubriceerde EU-informatie door de contractant of subcontractant te worden beschermd.
22. De voorwaarden waaronder een contractant een beroep kan doen op subcontractanten, worden in de uitnodiging tot inschrijving en het contract omschreven.
23. Een contractant dient van de EDEO als aanbestedende instantie toestemming te krijgen voordat hij delen van een gerubriceerde opdracht uitbestedt aan een subcontractant. Industriële of andere entiteiten die geregistreerd zijn in een land dat geen lidstaat van de Europese Unie is en geen informatiebeveiligingsovereenkomst met de Europese Unie heeft gesloten, mogen niet als subcontractant worden ingeschakeld.
24. Het is de verantwoordelijkheid van de contractant te garanderen dat alle onderaannemingsactiviteiten verlopen in overeenstemming met de minimumnormen van dit besluit; de contractant mag geen gerubriceerde EU-informatie aan een subcontractant doorgeven zonder voorafgaande schriftelijke toestemming van de aanbestedende instantie.
25. Wat betreft gerubriceerde EU-informatie die door de contractant of subcontractant wordt gegenereerd of verwerkt, oefent de aanbestedende instantie de rechten van de opsteller uit.

VI. BEZOEKEN IN VERBAND MET GERUBRICEERDE OPDRACHTEN

26. Wanneer de EDEO, contractanten of subcontractanten voor de uitvoering van een gerubriceerde opdracht op elkaars locaties toegang vragen tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET, worden in overleg met de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit bezoeken georganiseerd. Dit doet geen afbreuk aan het recht van de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit om in het kader van specifieke projecten een procedure overeen te komen waarmee zulke bezoeken rechtstreeks kunnen worden georganiseerd.
27. Alle bezoekers dienen over een passende veiligheidsmachtiging te beschikken en een noodzaak tot kennisname te hebben, alvorens zij toegang krijgen tot de gerubriceerde EU-informatie die betrekking heeft op de opdracht van de EDEO.
28. Bezoekers krijgen uitsluitend toegang tot de gerubriceerde EU-informatie die verband houdt met het doel van het bezoek.

VII. OVERDRACHT EN VERVOER VAN GERUBRICEERDE EU-INFORMATIE

29. Op de overdracht van gerubriceerde EU-informatie met elektronische middelen zijn de desbetreffende bepalingen van bijlage A, artikel 8, en bijlage A IV van toepassing.
30. Op het vervoer van gerubriceerde EU-informatie zijn de desbetreffende bepalingen van bijlage A III van toepassing, overeenkomstig de nationale wet- en regelgeving.
31. Wat het vervoer van gerubriceerd materiaal als vracht betreft, worden bij de opstelling van de beveiligingsregelingen de volgende beginselen toegepast:
 - a) de beveiliging wordt tijdens alle fasen van het vervoer gewaarborgd, van het punt van oorsprong tot de eindbestemming;
 - b) de mate van bescherming die aan een zending wordt verleend, wordt bepaald door de hoogste rubriceringsgraad van het materiaal dat zij bevat;
 - c) er moet een veiligheidsmachtiging voor een vestiging op het passende niveau worden verkregen voor de ondernemingen die het vervoer verzorgen, indien dat inhoudt dat gerubriceerde informatie in de vestigingen van de contractant worden opgeslagen. In ieder geval moeten de personeelsleden die de zending verwerken, in overeenstemming met bijlage A I een passende veiligheidsmachtiging hebben;

- d) vóór iedere grensoverschrijdende verplaatsing van materiaal met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL of SECRET UE/EU SECRET stelt de verzender een vervoersplan op, dat wordt goedgekeurd door de EDEO, in voorkomend geval in overleg met de betrokken nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit van zowel de verzender als de geadresseerde;
- e) het vervoer geschiedt zoveel mogelijk zonder onderbreking en wordt zo snel als de omstandigheden toelaten uitgevoerd;
- f) waar mogelijk leidt de route alleen door lidstaten. Routes door niet-lidstaten worden alleen gevolgd met toestemming van de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit of andere bevoegde veiligheidsautoriteit van de staat van de verzender en de staat van de geadresseerde.

VIII. OVERDRACHT VAN GERUBRICEERDE EU-INFORMATIE AAN CONTRACTANTEN IN DERDE STATEN

- 32. De overdracht van gerubriceerde EU-informatie aan contractanten en subcontractanten in derde staten die met de EU een geldige beveiligingsovereenkomst hebben, geschiedt overeenkomstig de beveiligingsmaatregelen die zijn overeengekomen door de EDEO als aanbestedende dienst en de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit van de derde staat waar de betrokken contractant is geregistreerd.

IX. BEHANDELING EN OPSLAG VAN INFORMATIE MET RUBRICERING RESTREINT UE/EU RESTRICTED

- 33. Waar nodig in samenwerking met de nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit van de lidstaat is de EDEO als aanbestedende instantie op basis van contractuele bepalingen gerechtigd bezoeken af te leggen aan vestigingen van contractanten/subcontractanten om na te gaan of passende beveiligingsmaatregelen zijn getroffen voor de bescherming van EU-informatie met rubricering RESTREINT UE/EU RESTRICTED, indien de opdracht zulks vereist.
- 34. Voor zover dat nodig is volgens de nationale wet- en regelgeving, worden nationale veiligheidsautoriteiten/aangewezen veiligheidsautoriteiten of andere bevoegde veiligheidsautoriteiten door de EDEO als aanbestedende dienst in kennis gesteld van opdrachten of opdrachten in onderaanneming die informatie met rubricering RESTREINT UE/EU RESTRICTED bevatten.
- 35. Een veiligheidsmachtiging voor een vestiging of veiligheidsmachtigingen voor het personeel van contractanten of subcontractanten is niet vereist voor opdrachten van de EDEO die informatie met rubricering RESTREINT UE/EU RESTRICTED bevatten.
- 36. De EDEO onderzoekt als aanbestedende dienst de reacties op de uitnodigingen tot inschrijving voor opdrachten waarvoor toegang tot informatie met rubricering RESTREINT UE/EU RESTRICTED nodig is, ongeacht eventuele vereisten met betrekking tot veiligheidsmachtigingen voor vestigingen of personen uit hoofde van de nationale wet- en regelgeving.
- 37. De voorwaarden voor uitbesteding in onderaanneming door de contractant zijn in overeenstemming met het bepaalde in de punten 22 tot en met 24.
- 38. Wanneer een opdracht de verwerking van informatie met rubricering RESTREINT UE/EU RESTRICTED in een door een contractant geëxploiteerd communicatie- en informatiesysteem behelst, ziet de EDEO er als aanbestedende dienst op toe dat in het contract of het contract inzake de onderaanneming de noodzakelijke technische en administratieve vereisten zijn opgenomen met betrekking tot de homologatie van het communicatie- en informatiesysteem in overeenstemming met het ingeschatte risico, rekening houdend met alle belangrijke factoren. Hoe ver de homologatie van een dergelijk communicatie- en informatiesysteem reikt, wordt door de aanbestedende dienst en de bevoegde nationale veiligheidsautoriteit/aangewezen veiligheidsautoriteit bepaald.

BIJLAGE A VI

UITWISSELING VAN GERUBRICEERDE INFORMATIE MET DERDE STATEN EN INTERNATIONALE ORGANISATIES

I. INLEIDING

1. Deze bijlage bevat bepalingen ter uitvoering van bijlage A, artikel 10.

II. KADERS VOOR DE UITWISSELING VAN GERUBRICEERDE INFORMATIE

2. De EDEO mag gerubriceerde EU-informatie uitwisselen met derde staten of internationale organisaties overeenkomstig bijlage A, artikel 10, lid 1.

Ter ondersteuning van de hoge vertegenwoordiger bij de uitvoering van diens taken uit hoofde van artikel 218 VWEU:

- a) stelt de betrokken geografische of thematische dienst van de EDEO in overleg met het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, in voorkomend geval vast of met de betrokken derde staat of internationale organisatie langdurige uitwisseling van gerubriceerde EU-informatie vereist is;
 - b) dient het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, in overleg met de betrokken geografische dienst van de EDEO in voorkomend geval bij de hoge vertegenwoordiger ontwerp teksten in voorstellen die aan de Raad worden voorgelegd krachtens artikel 218, leden 3, 5 en 6, VWEU;
 - c) biedt het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, de hoge vertegenwoordiger ondersteuning bij onderhandelingen, in coördinatie met de betrokken diensten van de Commissie en het secretariaat-generaal van de Raad;
 - d) dient het directoraat Crisisbeheersing en Planning van de EDEO met betrekking tot overeenkomsten of regelingen met derde staten betreffende hun deelname aan GVDB-crisisbeheersingsoperaties als bedoeld in bijlage A, artikel 10, lid 1, onder c), in overleg met de betrokken diensten van de EDEO, in voorkomend geval bij de hoge vertegenwoordiger ontwerp teksten in voorstellen die aan de Raad worden voorgelegd krachtens artikel 218, leden 3, 5 en 6, VWEU, en biedt dit directoraat de hoge vertegenwoordiger ondersteuning bij onderhandelingen, in coördinatie met de betrokken diensten van de EDEO en het secretariaat-generaal van de Raad.
3. Indien een informatiebeveiligingsovereenkomst voorziet in een technische uitvoeringsregeling, overeen te komen door het directoraat van de EDEO dat verantwoordelijk is voor beveiliging (in coördinatie met het directoraat Beveiliging van het directoraat-generaal Personele Middelen en Veiligheid van de Commissie en de dienst Beveiliging van het secretariaat-generaal van de Raad) en de bevoegde veiligheidsautoriteit van de betrokken derde staat of internationale organisatie, wordt in die regeling rekening gehouden met het beschermingsniveau dat door de beveiligingsvoorschriften, -structuren en -procedures van die derde staat of internationale organisatie wordt geboden.
 4. Wanneer het noodzakelijk is dat de EDEO met een derde staat of internationale organisatie gedurende lange tijd informatie uitwisselt met een rubriceringsgraad die niet hoger is dan RESTREINT UE/EU RESTRICTED, en is vastgesteld dat de partij in kwestie geen beveiligingssysteem heeft dat voldoende is ontwikkeld om een informatiebeveiligingsovereenkomst te sluiten, mag de hoge vertegenwoordiger, na een unaniem gunstig advies van het Beveiligingscomité van de EDEO overeenkomstig artikel 15, lid 5, van dit besluit, met de bevoegde veiligheidsautoriteiten van de derde staat of de internationale organisatie in kwestie een administratieve regeling treffen.
 5. Met derde staten of internationale organisaties mag geen gerubriceerde EU-informatie worden uitgewisseld met elektronische middelen, tenzij daarin in de informatiebeveiligingsovereenkomst of de administratieve regeling uitdrukkelijk is voorzien.
 6. In het kader van een administratieve regeling betreffende de uitwisseling van gerubriceerde informatie wijst zowel de EDEO als de betrokken derde staat of internationale organisatie een register aan als belangrijkste doorgangspunt voor de uitwisseling van gerubriceerde informatie. Voor de EDEO is dit het centrale register van de EDEO.
 7. Administratieve regelingen nemen als algemene regel de vorm van een briefwisseling aan.

III. EVALUATIEBEZOeken

8. De in artikel 17 van dit besluit bedoelde evaluatiebezoeken worden uitgevoerd in wederzijds overleg met de betrokken derde staat of internationale organisatie en dienen ter evaluatie van:
- a) het regelgevingskader voor de bescherming van gerubriceerde informatie;
 - b) specifieke kenmerken van de wet- en regelgeving, het beleid en de procedures op beveiligingsgebied van de betrokken derde staat of de internationale organisatie die van invloed kunnen zijn op de hoogste rubriceeringsgraad van de gerubriceerde informatie die kan worden uitgewisseld;
 - c) de vigerende beveiligingsmaatregelen en -procedures voor de bescherming van gerubriceerde informatie, en
 - d) de veiligheidsmachtigingsprocedures voor het vrij te geven niveau van gerubriceerde EU-informatie.
9. Er wordt geen gerubriceerde EU-informatie uitgewisseld voordat een evaluatiebezoek heeft plaatsgevonden en is vastgesteld op welk niveau gerubriceerde informatie tussen de partijen mag worden uitgewisseld, op basis van de gelijkwaardigheid van de bescherming die zal worden toegepast.

Indien de hoge vertegenwoordiger, voordat het evaluatiebezoek heeft plaatsgevonden, kennis neemt van uitzonderlijke of dringende redenen voor het uitwisselen van gerubriceerde informatie, handelt de EDEO als volgt:

- a) de EDEO vraagt ten eerste schriftelijke toestemming aan de opsteller van de informatie, om er zeker van te zijn dat deze geen bezwaar heeft tegen de vrijgave;
- b) de EDEO verwijst de zaak naar de veiligheidsautoriteit van de EDEO, die tot vrijgave kan beslissen mits daartoe van de in het Beveiligingscomité van de EDEO vertegenwoordigde lidstaten een unaniem gunstig advies is verkregen.

Indien de EDEO niet in staat is vast te stellen wie de opsteller is, neemt de veiligheidsautoriteit van de EDEO de verantwoordelijkheid van de opsteller op zich, nadat zij daartoe van het Beveiligingscomité van de EDEO een unaniem gunstig advies heeft verkregen.

IV. BEVOEGDHEID OM GERUBRICEERDE EU-INFORMATIE VRIJ TE GEVEN AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES

10. Wanneer er een kader bestaat voor de uitwisseling van gerubriceerde informatie met een derde staat of internationale organisatie, als bedoeld in bijlage A, artikel 10, lid 1, wordt het besluit waarbij de EDEO gerubriceerde EU-informatie vrijgeeft aan een derde staat of internationale organisatie genomen door de veiligheidsautoriteit van de EDEO, die deze toestemming mag delegeren aan hogere EDEO-ambtenaren of andere personen die onder haar gezag vallen.
11. Indien de vrij te geven gerubriceerde informatie of het bronnenmateriaal dat eventueel in die informatie is vervat niet afkomstig is van de EDEO, vraagt de EDEO vóór vrijgave schriftelijke toestemming aan de opsteller, om er zeker van te zijn dat deze geen bezwaar heeft tegen de vrijgave. Indien de EDEO niet in staat is vast te stellen wie de opsteller is, neemt de veiligheidsautoriteit van de EDEO de verantwoordelijkheid van de opsteller op zich, nadat zij daartoe van de in het Beveiligingscomité van de EDEO vertegenwoordigde lidstaten een unaniem gunstig advies heeft verkregen.

V. UITZONDERLIJKE AD-HOCVRIJGAVE VAN GERUBRICEERDE EU-INFORMATIE

12. Indien een van de in bijlage A, artikel 10, lid 1, bedoelde kaders ontbreekt, en de belangen van de EU of van een of meer van haar lidstaten vereisen dat om dringende redenen van politieke of operationele aard gerubriceerde EU-informatie wordt vrijgegeven, mag bij wijze van uitzondering gerubriceerde EU-informatie worden vrijgegeven aan een derde staat of internationale organisatie nadat een van de volgende maatregelen is getroffen.

Het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, handelt als volgt, nadat het zich ervan heeft vergewist dat aan de voorwaarden van punt 11 is voldaan:

- a) het gaat, voor zover mogelijk, met de veiligheidsautoriteiten van de betrokken derde staat of internationale organisatie na of de beveiligingsvoorschriften, -structuren en -procedures van die staat of organisatie van dien aard zijn dat aan hen vrijgegeven gerubriceerde EU-informatie wordt beschermd volgens normen die niet minder streng zijn dan die van dit besluit;

- b) het verzoekt het Beveiligingscomité van de EDEO om op basis van de beschikbare informatie advies uit te brengen over het vertrouwen dat kan worden gesteld in de beveiligingsvoorschriften, -structuren en -procedures van de derde staat of de internationale organisatie waaraan de gerubriceerde EU-informatie moet worden vrijgegeven;
 - c) de EDEO verwijst de zaak naar de veiligheidsautoriteit van de EDEO, die tot vrijgave kan beslissen mits daartoe van de in het Beveiligingscomité van de EDEO vertegenwoordigde lidstaten een unaniem gunstig advies is verkregen.
13. Indien een van de in bijlage A, artikel 10, lid 1, bedoelde kaders ontbreekt, verbindt de betrokken derde partij zich er schriftelijk toe de gerubriceerde EU-informatie op passende wijze te beschermen.
-

Aanhangsel A

Definities

Voor de toepassing van dit besluit wordt verstaan onder:

„homologatie”: het proces dat leidt tot de formele verklaring van de instantie voor veiligheidshomologatie (hierna „SAA” genoemd) dat een systeem mag functioneren met een bepaald rubriceringsniveau, in een specifieke beveiligingsmodus in zijn operationele omgeving en op een aanvaardbaar risiconiveau, nadat is vastgesteld dat een goedgekeurde reeks technische, fysieke, organisatorische en procedurele beveiligingsmaatregelen is geïmplementeerd;

„kritisch bestanddeel”: alles wat van waarde is voor een organisatie, haar bedrijfsactiviteiten en de continuïteit daarvan, met inbegrip van informatiebronnen ter ondersteuning van de opdracht van de organisatie;

„machtiging voor toegang tot gerubriceerde EU-informatie”: een machtiging die door de veiligheidsautoriteit van de EDEO overeenkomstig dit besluit wordt verleend nadat de bevoegde instanties van een lidstaat een veiligheidsmachtiging voor personen hebben afgegeven, waarbij wordt bevestigd dat de betrokkene, mits zijn „noodzaak tot kennisname” is vastgesteld, tot een bepaalde datum toegang kan krijgen tot gerubriceerde EU-informatie tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger) — zie bijlage A I, artikel 2;

„inbreuk”: het resultaat van iemands handeling of nalatigheid in strijd met de beveiligingsvoorschriften van dit besluit en/of het beveiligingsbeleid of de beveiligingsrichtsnoeren die maatregelen voor de uitvoering van dit besluit omvatten;

„levenscyclus van een communicatie- en informatiesysteem”: de volledige bestaansduur van een communicatie- en informatiesysteem, dat wil zeggen ingebruikname, conceptie, planning, behoefteanalyse, ontwerp, ontwikkeling, testen, implementatie, in bedrijf zijn, onderhoud en buitengebruikstelling;

„gerubriceerde opdracht”: een overeenkomst tussen de EDEO en een contractant voor de levering van goederen, de uitvoering van werken of de verlening van diensten waarvan de uitvoering de toegang tot of het genereren van gerubriceerde EU-informatie vereist of behelst;

„gerubriceerde onderaanneming”: een overeenkomst tussen een contractant van de EDEO en een andere contractant (de subcontractant) voor de levering van goederen, de uitvoering van werken of de verlening van diensten waarvan de uitvoering de toegang tot of het genereren van gerubriceerde EU-informatie vereist of behelst;

„communicatie- en informatiesysteem”: een systeem waarmee informatie in elektronische vorm kan worden verwerkt. Een communicatie- en informatiesysteem omvat alle onderdelen die voor het functioneren ervan vereist zijn, waaronder infrastructurele, organisatorische, personele en informatiemiddelen — zie bijlage A, artikel 8, lid 2;

„compromittering van gerubriceerde EU-informatie”: de volledige of gedeeltelijke bekendmaking van gerubriceerde EU-informatie aan onbevoegde personen of entiteiten — zie artikel 9, lid 2;

„contractant”: een natuurlijke persoon of een rechtspersoon die handelingsbekwaam is om overeenkomsten te sluiten;

„encryptieproducten”: encryptiealgoritmen, cryptografische hard- en softwaremodules en producten die nadere informatie betreffende de implementatie en bijbehorende documentatie en bedieningsmateriaal bevatten;

„EVDB-operatie”: een militaire of civiele crisisbeheersingsoperatie uit hoofde van titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie;

„derubricering”: de opheffing van een rubricering;

„defence in depth”: de toepassing van een reeks beveiligingsmaatregelen in de vorm van meerdere verdedigingslagen;

„aangewezen veiligheidsautoriteit”: (hierna „DSA” genoemd) een autoriteit onder het gezag van de nationale veiligheidsautoriteit (hierna „NSA” genoemd) van een lidstaat die tot taak heeft industriële of andere entiteiten te informeren over alle aspecten van het nationale beleid inzake industriële veiligheid, en leiding te geven en bijstand te verlenen bij de uitvoering ervan. De nationale veiligheidsautoriteit of een andere bevoegde instantie kan de rol van aangewezen veiligheidsautoriteit op zich nemen;

„document”: opgeslagen informatie, ongeacht de fysieke vorm of de kenmerken daarvan;

„verlagen van de rubricering”: verlaging van de rubriceringsgraad;

„gerubriceerde EU-informatie”: informatie of materiaal met een bepaalde EU-rubricering, waarvan de ongeoorloofde openbaarmaking de belangen van de Europese Unie of van een of meer van haar lidstaten in meerdere of mindere mate kan schaden — zie artikel 2, onder f);

„veiligheidsmachtiging voor een vestiging”: een administratieve beslissing van een nationale veiligheidsautoriteit of aangewezen veiligheidsautoriteit waaruit blijkt dat de vestiging vanuit beveiligingsoogpunt een afdoende niveau van bescherming biedt voor gerubriceerde EU-informatie met een bepaalde rubriceringsgraad, en dat alle personeelsleden die toegang tot gerubriceerde EU-informatie moeten hebben, een passend veiligheidsonderzoek hebben ondergaan en geïnstrueerd zijn over de toepasselijke beveiligingseisen die nodig zijn om gerubriceerde EU-informatie te kunnen raadplegen en beschermen;

„behandeling”: van gerubriceerde EU-informatie alle mogelijke handelingen waaraan gerubriceerde EU-informatie tijdens de gehele levenscyclus ervan kan worden onderworpen. Hiertoe behoren het genereren, verwerken, vervoeren, verlagen van de rubricering, declassificeren en vernietigen van de informatie. Met betrekking tot communicatie- en informatiesystemen behoort hiertoe ook het verzamelen, tonen, overdragen en opslaan ervan;

„houder”: een naar behoren gemachtigde persoon van wie de noodzaak tot kennisname vaststaat en die gerubriceerde EU-informatie in zijn bezit heeft en derhalve voor de bescherming daarvan verantwoordelijk is;

„industriële of andere entiteit”: een entiteit die betrokken is bij de levering van goederen, de uitvoering van werken of de verlening van diensten; het kan hierbij gaan om entiteiten die actief zijn op het gebied van industrie, handel, diensten, wetenschap, onderzoek, onderwijs of ontwikkeling, of om een zelfstandige;

„industriële beveiliging”: de toepassing van maatregelen om de bescherming van gerubriceerde EU-informatie door contractanten of subcontractanten tijdens precontractuele onderhandelingen en tijdens de volledige looptijd van gerubriceerde opdrachten te waarborgen — zie bijlage A, artikel 9, lid 1;

„information assurance” (IA): op het gebied van communicatie- en informatiesystemen het vertrouwen dat die systemen de erin opgenomen informatie zullen beschermen en zullen functioneren zoals nodig en wanneer nodig, onder de controle van legitieme gebruikers. Doeltreffende IA waarborgt passende niveaus van vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid en authenticiteit. IA is op een risicobeheersingsproces gebaseerd — zie bijlage A, artikel 8, lid 1;

„interconnectie”: een rechtstreekse koppeling van twee of meer IT-systemen, met als doel het gezamenlijk gebruik van informatie en andere bronnen van informatie (bijvoorbeeld communicatie), in één of meer richtingen — zie bijlage A IV, punt 31;

„beheer van gerubriceerde informatie”: het toepassen van administratieve maatregelen voor het controleren van gerubriceerde EU-informatie gedurende de gehele levenscyclus ervan, teneinde de in de artikelen 5, 8 en 6 bedoelde maatregelen aan te vullen, en daarbij het al dan niet opzettelijk compromitteren of verliezen van die informatie te helpen voorkomen, opsporen en herstellen. Die maatregelen hebben met name betrekking op het genereren, registreren, kopiëren, vertalen, vervoeren, verwerken, opslaan en vernietigen van gerubriceerde EU-informatie — zie bijlage A, artikel 7, lid 1;

„materiaal”: documenten of enigerlei onderdeel van machines of uitrusting die zijn of worden vervaardigd;

„opsteller”: de instelling, het orgaan of de instantie of de lidstaat van de EU, een derde staat of een internationale organisatie onder het gezag waarvan gerubriceerde informatie is gegenereerd en/of ingevoerd in de structuren van de EU;

„persoonsgerelateerde beveiliging”: de toepassing van maatregelen die ervoor moeten zorgen dat toegang tot gerubriceerde EU-informatie uitsluitend wordt verleend aan personen die:

- een „noodzaak tot kennisname” hebben,
- wat de toegang tot informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger betreft, een veiligheidsmachtiging voor het passende niveau hebben of anderszins uit hoofde van hun functie daartoe naar behoren zijn gemachtigd in overeenstemming met de nationale wet- en regelgeving, en
- zijn geïnstrueerd over hun verantwoordelijkheden —

zie bijlage A, artikel 5, lid 1;

„veiligheidsmachtiging voor personen”: voor toegang tot gerubriceerde EU-informatie een verklaring van een bevoegde autoriteit van een lidstaat die wordt afgegeven na voltooiing van een veiligheidsonderzoek door de bevoegde autoriteiten van die lidstaat, waarbij wordt bevestigd dat de betrokkene, op voorwaarde dat zijn „noodzaak tot kennisname” is vastgesteld, tot een bepaalde datum toegang mag hebben tot gerubriceerde EU-informatie tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger); van die persoon wordt dan gezegd dat hij „gecleard” is;

„certificaat van veiligheidsmachtiging voor personen” een door een bevoegde autoriteit afgegeven certificaat voor toegang tot gerubriceerde EU-informatie waarin wordt bevestigd dat een betrokkene in het bezit is van een geldige veiligheidsmachtiging voor personen of van een geldige veiligheidsmachtiging van het hoofd van het directoraat van de EDEO dat verantwoordelijk is voor beveiliging, en dat de rubriceringsgraad vermeldt van gerubriceerde EU-informatie waartoe hij toegang mag hebben (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger), alsook de geldigheidsduur van de relevante veiligheidsverklaring of -machtiging en de datum waarop de geldigheid van het certificaat zelf afloopt;

„fysieke beveiliging”: de toepassing van fysieke en technische beschermingsmaatregelen om toegang zonder machtiging tot gerubriceerde EU-informatie te ontmoedigen — zie bijlage A, artikel 6;

„programma-/projectbeveiligingsinstructie”: een lijst van beveiligingsprocedures die op een specifiek programma/project worden toegepast om de beveiligingsprocedures te standaardiseren. Deze kan gedurende de gehele looptijd van het programma/project worden herzien;

„registratie”: de toepassing van procedures waarbij de levenscyclus van materiaal, met inbegrip van de verspreiding en de vernietiging ervan, wordt geregistreerd — zie bijlage A III, punt 21;

„residueel risico”: het risico dat blijft bestaan nadat er beveiligingsmaatregelen zijn genomen, aangezien niet alle dreigingen worden ondervangen en niet alle kwetsbaarheden kunnen worden weggenomen;

„risico”: de mogelijkheid dat een bepaalde dreiging de interne en externe kwetsbaarheden van een organisatie of een van de door haar gebruikte systemen zal uitbuiten en daarbij schade zal toebrengen aan de organisatie en haar materiële en immateriële kritische bestanddelen. Risico wordt gemeten als een combinatie van de waarschijnlijkheid dat dreigingen zich zullen voordoen en het effect daarvan;

„risicoaanvaarding”: het besluit om erin te berusten dat er na de risicobehandeling een residueel risico blijft bestaan;

„risicobeoordeling”: het in kaart brengen van dreigingen en kwetsbaarheden en het verrichten van de daarmee verband houdende risicoanalyse, dat wil zeggen analyse van de waarschijnlijkheid en het effect;

„risicocommunicatie”: houdt in dat er risicovoorlichtingscampagnes worden gevoerd, gericht op gebruikers van communicatie- en informatiesystemen, dat goedkeuringsautoriteiten over die risico's worden geïnformeerd en dat er verslag over wordt uitgebracht aan de exploitanten;

„risicobeheersingsproces”: het volledige proces van het vaststellen, onder controle houden en tot een minimum beperken van onzekere gebeurtenissen die de veiligheid van een organisatie of de door haar gebruikte systemen kunnen treffen. Het bestrijkt alle risicogebonden activiteiten, met inbegrip van beoordeling, behandeling, aanvaarding en communicatie;

„risicobehandeling”: het matigen, verwijderen, verkleinen (via een passende combinatie van technische, fysieke, organisatorische of procedurele maatregelen), overbrengen of onder toezicht houden van het risico;

„memorandum over beveiligingsaspecten”: een geheel van bijzondere, door de aanbestedende instantie uitgevaardigde contractvoorwaarden die een integrerend deel uitmaken van een gerubriceerde opdracht die de toegang tot of het genereren van gerubriceerde EU-informatie behelst, en waarin de beveiligingseisen of de te beveiligen elementen van de opdracht worden beschreven;

„rubriceringsgids”: een document waarin wordt bepaald welke elementen van een programma of opdracht gerubriceerd zijn en wat de toepasselijke rubriceringsgraden zijn. De rubriceringsgids kan gedurende de looptijd van het programma of de opdracht worden uitgebreid en de informatie kan opnieuw of lager worden gerubriceerd; als er een rubriceringsgids is, is deze onderdeel van het memorandum over beveiligingsaspecten — zie bijlage A V, afdeling II;

„veiligheidsonderzoek”: de onderzoeksprocedures die de bevoegde autoriteit van een lidstaat overeenkomstig de nationale wet- en regelgeving uitvoert om zekerheid te krijgen dat er geen negatieve feiten bekend zijn waardoor de betrokkene niet in aanmerking zou komen voor een nationale of EU-veiligheidsmachtiging voor personen voor toegang tot gerubriceerde EU-informatie tot op een bepaald niveau (CONFIDENTIEL UE/EU CONFIDENTIAL of hoger);

„operationele beveiligingsprocedures”: een omschrijving van de te kiezen implementatie van het veiligheidsbeleid, de te volgen operationele procedures en de verantwoordelijkheden van het personeel;

„gevoelige niet-gerubriceerde informatie”, dat wil zeggen informatie die of materiaal dat de EDEO moet beschermen vanwege wettelijke verplichtingen op grond van de Verdragen of op grond van rechtshandelingen ter uitvoering van de Verdragen, en/of vanwege hun gevoelige karakter. Gevoelige niet-gerubriceerde informatie omvat, maar is niet beperkt tot, informatie of materiaal waarop de geheimhoudingsplicht van toepassing is, als bedoeld in artikel 339 VWEU, informatie die wordt gedekt door de belangen die worden beschermd bij artikel 4 van Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad ⁽¹⁾, in samenhang met de relevante jurisprudentie van het Hof van Justitie van de Europese Unie, of persoonsgegevens als bedoeld in Verordening (EG) nr. 45/2001.

„specifieke verklaring van beveiligingseisen”: een bindend geheel van beveiligingsbeginselen die in acht moeten worden genomen en gedetailleerde beveiligingseisen die moeten worden geïmplementeerd, dat ten grondslag ligt aan het proces van de certificatie en homologatie van communicatie- en informatiesystemen;

„TEMPEST”: het onderzoeken en bestuderen van en het toezicht houden op compromitterende elektromagnetische emissies en de maatregelen om deze te bestrijden;

„(be)dreiging”: een mogelijke oorzaak van een ongewenst incident dat kan leiden tot schade aan een organisatie of de door haar gebruikte systemen; zulke (be)dreigingen kunnen onopzettelijk of opzettelijk (kwaadwillig) zijn, en worden gekenmerkt door bedreigende elementen, mogelijke doelwitten en aanvalsmethoden;

„kwetsbaarheid”: een zwakte van welke aard dan ook die door een of meer (be)dreigingen kan worden uitgebuit. Kwetsbaarheid kan bestaan in nalatigheid of kan verband houden met onvoldoende strenge, onvolledige of onsamenvangende controles en kan van technische, procedurele, fysieke, organisatorische of operationele aard zijn.

⁽¹⁾ Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

Aanhangsel B

Concordantie van de beveiligingsrubriceringen

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
België	Très Secret (Loi 11.12.1998) Zeër Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota ⁽¹⁾ below
Bulgarije	Строго секретно	Секретно	Поверително	За служебно ползване
Tsjechië	Prísne tajné	Tajné	Důvěrné	Vyhrazené
Denemarken	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Duitsland	STRENG GEHEIM	GEHEIM	VS ⁽²⁾ — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ierland	Top Secret	Secret	Confidential	Restricted
Griekenland	Άκρως Απόρρητο Afkorting: ΑΑΠ	Απόρρητο Afkorting: (ΑΠ)	Εμπιστευτικό Afkorting: (ΕΜ)	Περιορισμένης Χρήσης Afkorting: (ΠΧ)
Spanje	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankrijk	Très Secret Défense	Secret Défense	Confidentiel Défense	nota ⁽³⁾ below
Kroatië	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italië	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Afkorting: (ΑΑΠ)	Απόρρητο Afkorting: (ΑΠ)	Εμπιστευτικό Afkorting: (ΕΜ)	Περιορισμένης Χρήσης Afkorting: (ΠΧ)
Letland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litouwen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongarije	„Szigorúan titkos!”	„Titkos!”	„Bizalmas!”	„Korlátozott terjesztésű!”
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederland	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Oostenrijk	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roemenië	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenië	Strogo tajno	Tajno	Zaupno	Interno
Slowakije	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Zweden ⁽⁴⁾	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Verenigd Koninkrijk	UK TOP SECRET	UK SECRET	Geen equivalent ⁽⁵⁾	UK OFFICIAL — SENSITIVE

⁽¹⁾ Diffusion Restreinte/Beperkte Verspreiding bestaat in België niet als rubricering. België behandelt en beschermt alle gegevens met rubricering „RESTREINT UE/ EU RESTRICTED” op een niet minder stringente wijze dan door de normen en procedures in beveiligingsvoorschriften van de Raad van de Europese Unie wordt voorgeschreven.

⁽²⁾ Duitsland: VS = Verschlusssache.

⁽³⁾ Frankrijk maakt in zijn nationale systeem geen gebruik van de rubricering „RESTREINT”. Frankrijk behandelt en beschermt alle gegevens met rubricering „RESTREINT UE/EU RESTRICTED” op een niet minder stringente wijze dan door de normen en procedures in de beveiligingsvoorschriften van de Raad van de Europese Unie wordt voorgeschreven.

⁽⁴⁾ Zweden: de rubriceringen op de bovenste rij worden gebruikt door de defensieautoriteiten en die op de onderste rij door andere instanties.

⁽⁵⁾ Het Verenigd Koninkrijk behandelt en beschermt alle gerubriceerde EU-informatie met de rubricering „CONFIDENTIEL UE/EU CONFIDENTIAL” overeenkomstig de beveiligingsvoorschriften die gelden voor „UK SECRET”.

ISSN 1977-0995 (elektronische uitgave)
ISSN 1725-2474 (papieren uitgave)



Bureau voor publicaties van de Europese Unie
2985 Luxemburg
LUXEMBURG

NL