Dit document vormt slechts een documentatiehulpmiddel en verschijnt buiten de verantwoordelijkheid van de instellingen

►**B**

BESLUIT VAN DE COMMISSIE

van 29 november 2001

tot wijziging van haar reglement van orde

(kennisgeving geschied onder nummer C(2001) 3031)

(2001/844/EG, EGKS, Euratom)

(PB L 317 van 3.12.2001, blz. 1)

Gewijzigd bij:

		Publicatieblad		
		nr.	blz.	datum
►**M1**	Besluit 2005/94/EG, Euratom van de Commissie van 3 februari 2005	L 31	66	4.2.2005
►**M2**	Besluit 2006/70/EG, Euratom van de Commissie van 31 januari 2006	L 34	32	7.2.2006
►**M3**	Besluit 2006/548/EG, Euratom van de Commissie van 2 augustus 2006	L 215	38	5.8.2006
►**M4**	Verordening (EU) nr. 519/2013 van de Commissie van 21 februari 2013	L 158	74	10.6.2013

▼B

BESLUIT VAN DE COMMISSIE

van 29 november 2001

tot wijziging van haar reglement van orde

(kennisgeving geschied onder nummer C(2001) 3031)

(2001/844/EG, EGKS, Euratom)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 218, lid 2,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap voor Kolen en Staal, en met name op artikel 16,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie, en met name op artikel 131,

Gelet op het Verdrag tot oprichting van de Europese Unie, en met name op artikel 28, lid 1, en artikel 41, lid 1,

BESLUIT:

Artikel 1

De veiligheidsvoorschriften van de Commissie, waarvan de tekst bij dit besluit is gevoegd, worden als bijlage toegevoegd aan het reglement van orde van de Commissie.

Artikel 2

Dit besluit treedt in werking op de dag van zijn bekendmaking in het *Publicatieblad van de Europese Gemeenschappen*.

Het is van toepassing vanaf 1 december 2001.

▼B

BIJLAGE

VEILIGHEIDSVOORSCHRIFTEN VAN DE COMMISSIE

Overwegende hetgeen volgt:

(1) Met het oog op de ontwikkeling van de werkzaamheden van de Commissie op gebieden die een zekere mate van vertrouwelijke behandeling vereisen, moet een integraal veiligheidssysteem worden opgezet dat geldt voor de Commissie, de krachtens of op basis van het EG-Verdrag of het Verdrag van de Europese Unie opgerichte andere instellingen, instanties, bureaus en agentschappen, de lidstaten en eventuele andere ontvangers van gerubriceerde informatie van de Europese Unie, hierna „gerubriceerde EU-gegevens" genoemd.

(2) Om de doeltreffendheid van het aldus opgezette veiligheidssysteem te waarborgen zal de Commissie gerubriceerde EU-gegevens uitsluitend ter beschikking stellen van die externe instanties die garanderen dat zij al het nodige hebben gedaan om bepalingen toe te passen die volstrekt gelijkwaardig zijn aan deze voorschriften.

(3) Deze voorschriften worden vastgesteld onverminderd Verordening nr. 3 van 31 juli 1958 ter toepassing van artikel 24 van het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie ([1]), Verordening (EEG) nr. 1588/90 van de Raad van 11 juni 1990 betreffende de toezending van onder de statistische geheimhoudingsplicht vallende gegevens aan het Bureau voor de Statistiek van de Europese Gemeenschappen ([2]) en Besluit C (95) 1510 def. van de Commissie van 23 november 1995 betreffende de bescherming van informatiesystemen.

(4) Met het oog op een vlot verloop van het besluitvormingsproces van de Unie wordt bij het opzetten van het veiligheidssysteem van de Commissie uitgegaan van de beginselen van Besluit 2001/264/EG van de Raad van 19 maart 2001 tot vaststelling van beveiligingsvoorschriften van de Raad ([3]).

(5) De Commissie onderstreept dat het van belang is dat de andere instellingen zo nodig worden betrokken bij de voorschriften en normen inzake vertrouwelijke behandeling die voor de bescherming van de belangen van de Unie en haar lidstaten nodig zijn.

(6) De Commissie erkent dat zij behoefte heeft aan een eigen veiligheidssysteem, rekening houdend met alle veiligheidsaspecten en het specifieke karakter van de Commissie als instelling.

(7) Deze voorschriften worden vastgesteld onverminderd artikel 255 van het Verdrag en 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 ([4]).

▼M2

(8) Deze bepalingen doen geen afbreuk aan artikel 286 van het Verdrag en aan 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 gegeven.

▼B

Artikel 1

De veiligheidsvoorschriften van de Commissie worden vastgesteld in de bijlage.

([1]) PB 17 van 6.10.1958, blz. 406/58.
([2]) PB L 151 van 15.6.1990, blz. 1.
([3]) PB L 101 van 11.4.2001, blz. 1.
([4]) PB L 145 van 31.5.2001, blz. 43.

▼B

Artikel 2

1. Het voor veiligheid bevoegde Commissielid neemt passende maatregelen om ervoor te zorgen dat de in artikel 1 bedoelde voorschriften bij de behandeling van gerubriceerde EU-gegevens worden nageleefd, zowel in de Commissie, door de ambtenaren en andere personeelsleden van de Commissie en het bij de Commissie gedetacheerde personeel, als in alle locaties van de Commissie, inclusief haar Vertegenwoordigingen en Bureaus in de Unie en haar Delegaties in derde landen, alsmede door de externe contractanten van de Commissie.

▼M3

Wanneer een opdracht of subsidieovereenkomst tussen de Commissie en een externe contractant of begunstigde de verwerking van gerubriceerde EU-gegevens in de locaties van de contractant of de begunstigde inhoudt, moeten de maatregelen die de externe contractant of begunstigde neemt om te waarborgen dat bij behandeling van gerubriceerde EU-gegevens de in artikel 1 bedoelde voorschriften worden nageleefd, een integrerend deel zijn van de opdracht of subsidieovereenkomst.

▼B

2. De lidstaten en de krachtens of op basis van de Verdragen opgerichte andere instellingen, instanties, bureaus en agentschappen worden gemachtigd gerubriceerde EU-gegevens te ontvangen op voorwaarde dat zij ervoor zorgen dat, wanneer gerubriceerde EU-gegevens worden behandeld, in hun diensten en locaties voorschriften worden toegepast die volstrekt gelijkwaardig zijn aan die als bedoeld in artikel 1, en met name door:

a) de leden van de permanente vertegenwoordigingen van de lidstaten bij de Europese Unie en de leden van de nationale delegaties die bijeenkomsten van de Commissie of van onder haar ressorterende instanties bijwonen, of deelnemen aan andere werkzaamheden van de Commissie,

b) de andere leden van de nationale overheden van de lidstaten die gerubriceerde EU-gegevens verwerken, hetzij op het grondgebied van de betrokken lidstaat hetzij daarbuiten,

c) de externe contractanten en gedetacheerde personeelsleden die gerubriceerde EU-gegevens verwerken.

Artikel 3

Derde landen, internationale organisaties en andere instanties worden gemachtigd gerubriceerde EU-gegevens te ontvangen op voorwaarde dat zij ervoor zorgen dat bij de behandeling van dergelijke gegevens, voorschriften worden nageleefd die volstrekt gelijkwaardig zijn aan die als bedoeld in artikel 1.

Artikel 4

In overeenstemming met de in deel I van de bijlage bedoelde grondbeginselen en minimumnormen inzake veiligheid kan het voor veiligheid bevoegde Commissielid maatregelen nemen overeenkomstig deel II van de bijlage.

Artikel 5

Deze voorschriften vervangen vanaf de dag van hun toepassing:

a) Besluit C (94) 3282 van 30 november 1994 betreffende de veiligheidsmaatregelen van toepassing op de gerubriceerde informatie die in het kader van de werkzaamheden van de Europese Unie wordt samengesteld of uitgewisseld;

b) Besluit C (99) 423 van 25 februari 1999 betreffende de regeling inzake de machtiging van ambtenaren en andere personeelsleden van de Europese Commissie tot raadpleging van gerubriceerde informatie die de Commissie in haar bezit heeft.

▼B

Artikel 6

Vanaf de datum van de toepassing van deze voorschriften geldt voor alle gerubriceerde gegevens die tot die datum in het bezit van de Commissie zijn, met uitzondering van de gerubriceerde gegevens van Euratom, het volgende:

a) als zij door de Commissie zijn gecreëerd, worden zij geacht automatisch te worden heringedeeld in de rubriek „►**M1** RESTREINT UE ◄”, tenzij de auteur uiterlijk op 31 januari 2002 besluit ze in een andere rubriek in te delen. In dit geval informeert de auteur alle geadresseerden van het betrokken document;

b) als zij door auteurs buiten de Commissie zijn gecreëerd, behouden zij hun oorspronkelijke rubricering en worden zij behandeld als gerubriceerde EU-gegevens van het overeenkomstige niveau, tenzij de auteur ermee instemt de gegevens in een lagere rubriek in te delen of de rubricering op te heffen.

▼B

BIJLAGE

VEILIGHEIDSVOORSCHRIFTEN

Inhoud

DEEL I:	**GRONDBEGINSELEN EN MINIMUMNORMEN INZAKE VEILIGHEID**
1.	INLEIDING
2.	ALGEMENE BEGINSELEN
3.	GRONDBEGINSELEN
4.	BEGINSELEN VAN DE GEGEVENSBEVEILIGING
4.1.	**Doelstellingen**
4.2.	**Definities**
4.3.	**Rubricering**
4.4.	**Doel van de veiligheidsmaatregelen**
5.	ORGANISATIE VAN DE BEVEILIGING
5.1.	**Gemeenschappelijke minimumnormen**
5.2.	**Organisatie**
6.	VEILIGHEID VAN HET PERSONEEL
6.1.	**Veiligheidsonderzoek van het personeel**
6.2.	**Machtigingsgegevens van het personneel**
6.3.	**Veiligheidsinstructies voor het personeel**
6.4.	**Beheersverantwoordelijkheden**
6.5.	**Veiligheidsstatus van het personeel**
7.	FYSIEKE BEVEILIGING
7.1.	**De noodzaak van bescherming**
7.2.	**Controle**
7.3.	**Beveiliging van gebouwen**
7.4.	**Calamiteitenplannen**
8.	INFORMATIEBEVEILIGING
9.	BEVEILIGING TEGEN SABOTAGE EN BESTRIJDING VAN ANDERE VORMEN VAN KWAADWILLIGE BESCHADIGING
10.	VRIJGAVE VAN GERUBRICEERDE GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES
DEEL II:	**ORGANISATIE VAN DE BEVEILIGING IN DE COMMISSIE**
11.	HET VOOR VEILIGHEID BEVOEGDE COMMISSIELID
12.	DE ADVIESGROEP VEILIGHEIDSBELEID VAN DE COMMISSIE
13.	DE ADVIESRAAD VEILIGHEIDSBELEID VAN DE COMMISSIE
14.	►**M2** HET DIRECTORAAT VEILIGHEID VAN DE COMMISSIE ◄
15.	VEILIGHEIDSINSPECTIES
16.	RUBRICERINGEN, BEVEILIGINGSINDICATOREN EN MARKERINGEN
16.1.	**Rubriceringsniveaus**

▼B

16.2. **Beveiligingsindicator**

16.3. **Markeringen**

16.4. **Aanbrengen van een rubricering**

16.5. **Aanbrengen van beveiligingsindicatoren**

17. RUBRICERINGSBEHEER

17.1. **Algemeen**

17.2. **Rubricering**

17.3. **Lagere rubricering en derubricering**

18. FYSIEKE BEVEILIGING

18.1. **Algemeen**

18.2. **Veiligheidseisen**

18.3. **Fysieke beveiligingsmaatregelen**

18.3.1. *Veiligheidszones*

18.3.2. *Administratieve zone*

18.3.3. *Controles bij in- en uitgaan*

18.3.4. *Bewakingspatrouilles*

18.3.5. *Beveiligingsopbergmiddelen en braakwerende ruimten*

18.3.6. *Sloten*

18.3.7. *Controle van sleutels en codecombinaties*

18.3.8. *Indringerdetectie-/signaleringssystemen*

18.3.9. *Goedgekeurde uitrusting*

18.3.10. *Fysieke bescherming van kopieermachines en faxapparaten*

18.4. **Bescherming tegen waarneming van buitenaf en afluisteren**

18.4.1. *Waarneming van buitenaf*

18.4.2. *Afluisteren*

18.4.3. *Binnenbrengen van elektronische registratieapparatuur*

18.5. **Technisch veilige zones**

19. ALGEMENE VOORSCHRIFTEN BETREFFENDE HET NEED-TO-KNOW-BEGINSEL EN HET VEILIGHEIDSONDERZOEK

19.1. **Algemeen**

19.2. **Specifieke voorschriften inzake de toegang tot als TRES SECRET UE/EU TOP SECRET gerubriceerde gegevens**

19.3. **Specifieke voorschriften inzake de toegang tot als SECRET UE of CONFIDENTIEL UE gerubriceerde gegevens**

19.4. **Specifieke voorschriften inzake de toegang tot als RESTREINT UE gerubriceerde gegevens**

19.5. **Overdracht**

19.6. **Speciale instructies**

▼B

20. PROCEDURE MET BETREKKING TOT HET VEILIGHEIDSONDERZOEK VOOR AMBTENAREN EN ANDERE PERSONEELSLEDEN VAN DE COMMISSIE

21. VERVAARDIGING, VERSPREIDING, OVERDRACHT, BEVEILIGING VAN KOERIERS, EXTRA KOPIEËN, VERTALINGEN EN UITTREKSEL VAN GERUBRICEERD EU-MATERIAAL

21.1. **Vervaardiging**

21.2. **Verspreiding**

21.3. **Overdracht van gerubriceerde EU-documenten**

21.3.1. *Verpakking, ontvangstbewijzen*

21.3.2. *Overdracht binnen een gebouw of een groep gebouwen*

21.3.3. *Overdracht binnen een land*

21.3.4. *Overdracht van de ene staat naar de andere*

21.3.5. *Overdracht van RESTREINT UE documenten*

21.4. **Veiligheidsonderzoek van koeriers**

21.5. **Elektronische en andere middelen van technische overdracht**

21.6. **Extra kopieën, vertalingen en uittreksels van gerubriceerde EU-documenten**

22. EUCI-REGISTERS, CONTROLES, ARCHIVERING EN VERNIETIGING VAN GERUBRICEERDE EU-GEGEVENS

22.1. **Plaatselijke registers van gerubriceerde EU-gegevens (EUCI-registers)**

22.2. **Het TRES SECRET UE/EU TOP SECRET-register**

22.2.1. *Algemeen*

22.2.2. *Het Centraal TRES SECRET UE/EU TOP SECRET-register*

22.2.3. *TRES SECRET UE/EU TOP SECRET-subregisters*

22.3. **Inventarisatie en controle van gerubriceerde EU-documenten**

22.4. **Archivering van gerubriceerde EU-gegevens**

22.5. **Vernietiging van gerubriceerde EU-gegevens**

22.6. **Vernietiging in noodgevallen**

23. VEILIGHEIDSMAATREGELEN VOOR SPECIFIEKE VERGADERINGEN DIE BUITEN DE COMMISSIE WORDEN GEHOUDEN EN WAARBIJ GERUBRICEERDE EU-GEGEVENS ZIJN BETROKKEN

23.1. **Algemeen**

23.2. **Verantwoordelijkheid**

23.2.1. ►M2 *Het directoraat Veiligheid van de Commissie* ◄

23.2.2. *Beveiligingsfunctionaris van de vergadering (Meeting Security Officer — MSO)*

23.3 **Veiligheidsmaatregelen**

23.3.1. *Veiligheidszones*

23.3.2. *Pasjes*

23.3.3. *Controle van foto- en audioapparatuur*

▼B

23.3.4. *Controle van aktetassen, draagbare computers en pakjes*

23.3.5. *Technische beveiliging*

23.3.6. *Documenten van delegaties*

23.3.7. *Veilig opbergen van documenten*

23.3.8. *Controle van ruimten*

23.3.9. *Verwijdering van afval van gerubriceerd EU-materiaal*

24 INBREUKEN OP DE VEILIGHEIDSVOORSCHRIFTEN EN COMPROMITTERING VAN GERUBRICEERDE EU-GEGEVENS

24.1. **Definities**

24.2. **Melding van inbreuken op veiligheidsvoorschriften**

24.3. **Gerechtelijke actie**

25. BESCHERMING VAN GERUBRICEERDE EU-GEGEVENS DIE VERWERKT WORDEN IN IT- EN COMMUNICATIESYSTEMEN

25.1. **Inleiding**

25.1.1. *Algemeen*

25.1.2. *Bedreigingen en kwetsbaarheden van systemen*

25.1.3. *Voornaamste doel van veiligheidsmaatregelen*

25.1.4. *Systeemgebonden specificatie van beveiligseisen (SSRS)*

25.1.5. *Beveiligingsmodi*

25.2. **Definities**

25.3. **Verantwoordelijkheden in verband met beveiliging**

25.3.1. *Algemeen*

25.3.2. *De Autoriteit voor veiligheidsaccreditatie (SAA)*

25.3.3. *De Infosec-autoriteit (IA)*

25.3.4. *Eigenaar technisch systeem (TSO)*

25.3.5. *De Informatie-eigenaar (IO)*

25.3.6. *Gebruikers*

25.3.7. *Infosec-opleiding*

25.4. **Niet-technische beveiligingsmaatregelen**

25.4.1. *Personeelsgerelateerde beveiliging*

25.4.2. *Fysieke beveiliging*

25.4.3. *Controle op de toegang tot een systeem*

25.5. **Technische beveiligingsmaatregelen**

25.5.1. *Beveiliging van informatie*

25.5.2. *Controle van en verantwoordelijkheid voor gegevens*

25.5.3. *Behandeling en controle van verwijderbare digitale opslagmedia*

▼B

25.5.4. *Derubricering en vernietiging van digitale opslagmedia*

25.5.5. *Communicatiebeveiliging*

25.5.6. *Installatie- en stralingsbeveiliging*

25.6. **Beveiliging tijdens verwerking**

25.6.1. *Operationele beveiligingsprocedures (SecOP's)*

25.6.2. *Bescherming van software/configuratiebeheer*

25.6.3. *Controle op de aanwezigheid van kwaadaardige software/ computervirussen*

25.6.4. *Onderhoud*

25.7. **Aankopen**

25.7.1. *Algemeen*

25.7.2. *Accreditatie*

25.7.3. *Beoordeling en certificatie*

25.7.4. *Routinecontrole van beveiligingsvoorzieningen met het oog op verlenging van de accreditatie*

25.8. **Tijdelijk of occasioneel gebruik**

25.8.1. *Beveiliging van microcomputers/personal computers*

25.8.2. *Gebruik van privé IT-apparatuur voor officiële Commissiewerkzaamheden*

25.8.3. *Gebruik van IT-apparatuur van een contractant of van een lidstaat voor officiële Commissiewerkzaamheden*

26. VRIJGAVE VAN GERUBRICEERDE EU-GEGEVENS AAN DERDE LANDEN OF INTERNATIONALE ORGANISATIES

26.1.1. *Principes van de vrijgave van gerubriceerde EU-gegevens*

26.1.2. *Graden*

26.1.3. *Veiligheidsovereenkomsten*

AANHANGSEL 1: VERGELIJKING VAN DE NATIONALE BEVEILIGINGSRUBRICERINGEN

AANHANGSEL 2: PRAKTISCHE RUBRICERINGSGIDS

AANHANGSEL 3: RICHTSNOEREN VOOR VRIJGAVE VAN GERUBRICEERDE EU-GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES: EERSTEGRAADSSAMENWERKING

AANHANGSEL 4: RICHTSNOEREN VOOR VRIJGAVE VAN GERUBRICEERDE EU-GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES: TWEEDEGRAADSSAMENWERKING

AANHANGSEL 5: RICHTSNOEREN VOOR VRIJAVE VAN GERUBRICEERDE EU-GEGEVENS AAN DERDE STATEN OF INTERNATIONELE ORGANISATIES: DERDEGRAADSSAMENWERKING

AANHANGSEL 6: LIJST VAN AFKORTINGEN

▼B

DEEL I: GRONDBEGINSELEN EN MINIMUMNORMEN INZAKE VEILIGHEID

1. INLEIDING

Deze voorschriften bevatten de grondbeginselen en minimumnormen inzake veiligheid die door de Commissie in al haar standplaatsen en door alle ontvangers van gerubriceerde EU-gegevens (EUCI) op passende wijze moeten worden nageleefd om de veiligheid te garanderen en ervoor te zorgen dat iedereen er zeker van kan zijn dat er een gemeenschappelijke norm voor de bescherming geldt.

2. ALGEMENE BEGINSELEN

Het veiligheidsbeleid van de Commissie maakt integraal deel uit van haar algemeen beleid inzake intern beheer en is dus gebaseerd op de beginselen van haar algemeen beleid.

Deze beginselen zijn: wettigheid, transparantie,verantwoordingsplicht en subsidiariteit (proportionaliteit).

Wettigheid houdt in dat de veiligheidsfuncties strikt binnen het geldende rechtskader moeten worden uitgeoefend en dat de regelgeving moet worden nageleefd. Voorts betekent dit beginsel dat de verantwoordelijkheden inzake veiligheid op adequate rechtsvoorschriften moeten worden gebaseerd. Het personeelsstatuut is volledig van toepassing, en met name artikel 17 inzake de verplichting van de personeelsleden om discretie in acht te nemen ten aanzien van de informatie van de Commissie, en titel VI inzake tuchtmaatregelen. Ten slotte houdt dit beginsel in dat inbreuken op de veiligheid waarvoor de Commissie bevoegd is, moeten worden behandeld op een wijze die strookt met het beleid van de Commissie inzake tuchtmaatregelen en met haar beleid inzake samenwerking met de lidstaten op strafrechtelijk gebied.

Transparantie houdt in dat alle veiligheidsvoorschriften en -bepalingen duidelijk moeten zijn, dat er een evenwicht moet zijn tussen de verschillende diensten en de verschillende gebieden (fysieke veiligheid versus bescherming van de gegevens, enz.) en dat een coherent en gestructureerd beleid inzake veiligheidsbewustzijn moet worden gevoerd. Voorts wijst dit beginsel op de behoefte aan duidelijke schriftelijke richtsnoeren voor de uitvoering van de veiligheidsmaatregelen.

Verantwoordingsplicht houdt in dat de verantwoordelijkheden op het gebied van de veiligheid duidelijk worden vastgesteld. Voorts wijst dit beginsel erop dat regelmatig moet worden nagegaan of deze verantwoordelijkheden correct worden uitgeoefend.

Subsidiariteit (of proportionaliteit) betekent dat de beveiliging op het laagst mogelijke niveau moet worden georganiseerd en zo dicht mogelijk bij de Directoraten-generaal en de diensten van de Commissie. Voorts houdt dit beginsel in dat de beveiligingsactiviteiten worden beperkt tot die gebieden waarvoor het werkelijk nodig is. Ten slotte betekent dit beginsel dat de veiligheidsmaatregelen in verhouding moeten staan tot de te beschermen belangen en tot de feitelijke of mogelijke bedreiging van deze belangen, zodat de bescherming van die aard is dat zij zo weinig mogelijk ontwrichting veroorzaakt.

3. GRONDBEGINSELEN

De fundamenten voor een goede beveiliging zijn:

a) de aanwezigheid in iedere lidstaat van een nationale veiligheidsinstantie die verantwoordelijk is voor:

   1. het verzamelen en registreren van inlichtingen over spionage, sabotage, terrorisme en andere subversieve activiteiten, en

   2. het informeren en adviseren van haar regeringen, en via hen de Commissie, over de aard van de bedreigingen voor de veiligheid en de middelen om zich daartegen te beschermen;

▼B

b) de aanwezigheid in iedere lidstaat en in de Commissie van een technische Infosec-autoriteit (IA) die met de betrokken veiligheidsautoriteit samenwerkt om informatie en advies te verschaffen over technische bedreigingen voor de veiligheid en de middelen om zich daartegen te beschermen;

c) regelmatige samenwerking tussen de regeringsdiensten en de betrokken diensten van de Europese instellingen om, naar gelang van het geval, besluiten te nemen of aanbevelingen te doen inzake:

1. de personen, gegevens en middelen die beschermd moeten worden, en

2. gemeenschappelijke normen voor de bescherming;

d) nauwe samenwerking tussen ►M2 het directoraat Veiligheid van de Commissie ◄ (CSO) en de veiligheidsdiensten van de andere Europese instellingen, alsmede het Veiligheidsbureau van de NAVO (NOS).

4. BEGINSELEN VAN DE GEGEVENSBEVEILIGING

4.1. **Doelstellingen**

Met de beveiliging worden de volgende hoofddoelstellingen beoogd:

a) beveiliging van gerubriceerde EU-gegevens (EUCI) tegen spionage, compromittering of openbaarmaking zonder machtiging;

b) bescherming van EU-gegevens die in communicatie- en informatiesystemen en -netwerken worden verwerkt, tegen gevaren wat betreft het vertrouwelijke karakter, de integriteit en de beschikbaarheid ervan;

c) beveiliging van de locaties van de Commissie waarin EU-gegevens zijn ondergebracht, tegen sabotage en kwaadwillige beschadiging;

d) in geval van mislukking: beoordeling van de aangerichte schade, beperking van de consequenties daarvan en vaststelling van herstelmaatregelen.

4.2. **Definities**

In deze voorschriften wordt verstaan onder:

a) „gerubriceerde EU-gegevens” (EUCI): gegevens en materiaal waarvan openbaarmaking zonder machtiging de belangen van de EU of van een of meer van haar lidstaten in meerdere of mindere mate zou kunnen schaden, ongeacht of dergelijke gegevens afkomstig zijn van de EU, de lidstaten, derde staten of internationale organisaties;

b) „document”: brief, nota, notulen, verslag, memorandum, signaal/boodschap, schets, foto, dia, film, kaart, grafische voorstelling, plattegrond, notitieboek, stencil, carbonpapier, schrijfmachine- of printerlint, tape, cassette, computerschijf, CD-ROM of enig ander fysiek medium waarop gegevens zijn opgeslagen;

c) „materiaal”: een document als bedoeld onder b), alsook enig uitrustingsonderdeel dat gefabriceerd is of wordt;

d) „need to know”: de noodzaak voor een beambte om, met het oog op de uitoefening van zijn functie of de vervulling van zijn taak, toegang te krijgen tot gerubriceerde EU-gegevens;

e) „machtiging”: een besluit van ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄ om een persoon tot op een bepaald niveau toegang tot EUCI te verlenen op basis van een positief resultaat van een veiligheidsonderzoek (doorlichting) dat door een nationale veiligheidsinstantie overeenkomstig nationale rechtsvoorschriften is uitgevoerd;

▼B

f) „rubricering”: de toekenning van een passend beveiligingsniveau aan gegevens waarvan de openbaarmaking zonder machtiging in mindere of meerdere mate nadelig zou kunnen zijn voor de belangen van de Commissie of de lidstaten;

g) „lagere rubricering” (downgrading): verlaging van het rubriceringsniveau;

h) „derubricering” (declassification): opheffing van een rubricering;

i) „opsteller”: gemachtigd auteur van een gerubriceerd document. In de Commissie kunnen afdelingshoofden hun personeelsleden machtigen om EUCI op te stellen;

j) „afdelingen van de Commissie”: afdelingen en diensten van de Commissie, met inbegrip van de kabinetten, in alle standplaatsen, inclusief het Gemeenschappelijk Centrum voor Onderzoek, de Vertegenwoordigingen en Bureaus in de Unie en de Delegaties in derde landen.

4.3. **Rubricering**

a) Op het gebied van geheimhouding zijn aandacht en ervaring vereist bij de selectie van te beschermen gegevens en materiaal en bij de beoordeling van de mate van bescherming die noodzakelijk is. Het is van fundamenteel belang dat de mate van bescherming overeenstemt met de veiligheidsgevoeligheid van de betrokken gegevens of het betrokken materiaal. Om te zorgen dat de informatiestroom soepel verloopt, moet het nodige worden gedaan om zowel te hoge als te lage rubricering te voorkomen.

b) Het rubriceringssysteem is het instrument waarmee aan deze beginselen gevolg wordt gegeven; een soortgelijk rubriceringssysteem moet worden gebruikt voor het plannen en organiseren van de bestrijding van spionage, sabotage, terrorisme en andere bedreigingen, zodat de grootste mate van bescherming wordt geboden aan de belangrijkste locaties die gerubriceerde gegevens bevatten, en binnen die locaties aan de gevoeligste elementen.

c) Voor de rubricering is alleen de opsteller van de gegevens verantwoordelijk.

d) Het rubriceringsniveau mag uitsluitend worden bepaald op basis van de inhoud van de gegevens.

e) Als verschillende reeksen gegevens worden bijeengebracht, moet op het geheel een rubriceringsniveau worden toegepast dat minstens even hoog is als de hoogste rubricering. Een gegevensverzameling kan evenwel een hogere rubricering krijgen dan de afzonderlijke bestanddelen.

f) De rubriceringen worden alleen toegekend als dit nodig is, en zolang als dit nodig is.

4.4. **Doel van de veiligheidsmaatregelen**

De veiligheidsmaatregelen moeten:

a) betrekking hebben op alle personen die toegang hebben tot gerubriceerde gegevens, alle dragers van gerubriceerde informatie en alle locaties waar zich dergelijke gegevens en belangrijke installaties bevinden;

b) zodanig zijn ontworpen dat gedetecteerd wordt wanneer iemand de veiligheid van gerubriceerde gegevens en van belangrijke installaties die gerubriceerde gegevens bevatten, in gevaar kan brengen, en moeten in de uitsluiting of verwijdering van een dergelijke persoon voorzien;

▼B

c) voorkomen dat een niet-gemachtigde persoon toegang krijgt tot gerubriceerde gegevens of installaties die deze gegevens bevatten;

d) ervoor zorgen dat gerubriceerde gegevens alleen verspreid worden op basis van het „need to know”-beginsel, dat fundamenteel is voor alle aspecten van de veiligheid;

e) waarborgen bieden voor de integriteit (d.w.z. het voorkomen van schending of van wijziging of verwijdering van gegevens zonder machtiging) en de beschikbaarheid (d.w.z. dat de toegang niet geweigerd wordt aan degene die de gegevens nodig heeft en tot toegang gemachtigd is) van alle gegevens, al dan niet gerubriceerd, en in het bijzonder van gegevens die in elektromagnetische vorm worden opgeslagen, verwerkt of verzonden.

5. ORGANISATIE VAN DE BEVEILIGING

5.1. **Gemeenschappelijke minimumnormen**

De Commissie zorgt ervoor dat de gemeenschappelijke minimumnormen inzake veiligheid in acht worden genomen door alle EUCI-ontvangers, zowel in de instelling als in de onder haar ressorterende instanties, bijv. alle afdelingen en contractanten, zodat gerubriceerde EU-gegevens kunnen worden doorgegeven in het vertrouwen dat zij elders met dezelfde zorg verwerkt zullen worden. Deze minimumnormen omvatten criteria voor het veiligheidsonderzoek van het personeel en procedures voor de bescherming van gerubriceerde EU-gegevens.

De Commissie verleent externe instanties alleen toegang tot EUCI op voorwaarde dat zij ervoor zorgen dat bij de behandeling van EUCI wordt voldaan aan voorschriften die minstens volstrekt gelijkwaardig zijn aan deze minimumnormen.

▼M3

Die minimumnormen zijn ook van toepassing wanneer de Commissie uit hoofde van een opdracht of subsidieovereenkomst bij industriële of andere entiteiten opdrachten plaatst voor taken die betrekking hebben op gerubriceerde EU-gegevens of voor taken die dergelijke gegevens noodzakelijk maken en/of bevatten: deze gemeenschappelijke minimumnormen zijn opgenomen in afdeling 27 van deel II.

▼B

5.2. **Organisatie**

Binnen de Commissie is de beveiliging op twee niveaus georganiseerd:

a) op het niveau van de Commissie als geheel is er ►M2 het directoraat Veiligheid van de Commissie ◄, met een autoriteit voor veiligheidsaccreditatie (SAA), die ook optreedt als Crypto-autoriteit (CrA) en TEMPEST-autoriteit (TA), en met een INFOSEC-autoriteit (IA) en één of meer centrale EUCI-registers, elk met één of meer functionarissen voor de registercontrole (RCO);

b) op het niveau van de afdelingen van de Commissie valt de veiligheid onder de bevoegdheid van één of meer plaatselijke veiligheidsfunctionarissen (LSO), één of meer centrale informatiebeveiligingsfunctionarissen (CISO), plaatselijke informatiebeveiligingsfunctionarissen (LISO) en plaatselijke EUCI-registers met één of meer functionarissen voor de registercontrole;

c) De centrale veiligheidsinstanties geven de plaatselijke veiligheidsinstanties praktische richtsnoeren.

6. VEILIGHEID VAN HET PERSONEEL

6.1. **Veiligheidsonderzoek van het personeel**

Alle personen die toegang moeten hebben tot als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens, moeten een passend onderzoek ondergaan alvorens die toegang wordt verleend. Een soortgelijk onderzoek is vereist voor personen die taken hebben op het gebied van de technische bediening of het onderhoud van communicatie- en informatiesystemen die gerubriceerde gegevens bevatten. Dit onderzoek is erop gericht te bepalen of deze personen:

a) van onbetwiste loyaliteit zijn;

▼B

b) een zodanig karakter en een zodanige discretie bezitten dat hun betrouwbaarheid op het stuk van het verwerken van gerubriceerde gegevens buiten kijf staat;

c) kwetsbaar zijn voor druk van externe of andere bronnen.

Bij het onderzoek moet bijzondere aandacht worden geschonken aan personen die:

d) toegang zullen krijgen tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens;

e) functies bekleden waarbij zij regelmatig toegang krijgen tot een aanzienlijke hoeveelheid als ►M1 SECRET UE ◄ gerubriceerde gegevens;

f) door hun functie speciale toegang hebben tot beveiligde communicatie- of informatiesystemen en daardoor de mogelijkheid hebben om zonder machtiging toegang te krijgen tot grote hoeveelheden gerubriceerde EU-gegevens of om door technische sabotage ernstige schade te berokkenen.

In de onder d), e) en f) bedoelde omstandigheden wordt zo veel mogelijk gebruik gemaakt van de techniek van het antecedentenonderzoek.

Wanneer personen van wie de „need to know" niet is vastgesteld, moeten werken in omstandigheden waarin zij toegang kunnen hebben tot gerubriceerde EU-gegevens (bv. bodes, veiligheidspersoneel, onderhouds- en schoonmaakpersoneel, enz.) moeten zij eerst een passend veiligheidsonderzoek ondergaan.

6.2. **Machtigingsgegevens van het personeel**

Alle afdelingen van de Commissie die gerubriceerde EU-gegevens verwerken of beveiligde communicatie- of informatiesystemen huisvesten, houden de machtigingsgegevens bij van het daartoe aangewezen personeel. Elke machtiging wordt geverifieerd telkens als moet worden gegarandeerd dat die passend is voor de vigerende taakomschrijving van die persoon; dit nieuwe onderzoek is prioritair wanneer nieuwe informatie wordt ontvangen die erop wijst dat de voortzetting van de taak bij gerubriceerde werkzaamheden niet langer strookt met de veiligheidsbelangen. De plaatselijke veiligheidsfunctionaris van de betrokken afdeling van de Commissie houdt de machtigingsgegevens bij die op zijn activiteitensector betrekking hebben.

6.3. **Veiligheidsinstructies voor het personeel**

Alle personeelsleden die werkzaam zijn in omstandigheden waarin zij toegang zouden kunnen krijgen tot gerubriceerde gegevens, moeten bij het opnemen van hun taak en vervolgens met regelmatige tussenpozen grondige instructies krijgen over de noodzaak van beveiliging en de procedures om die beveiliging door te voeren. Dergelijke personeelsleden moeten schriftelijk bevestigen dat zij onderhavige veiligheidsvoorschriften hebben gelezen en volledig hebben begrepen.

6.4. **Beheersverantwoordelijkheden**

Leidinggevenden zijn ertoe verplicht de leden van hun personeel die bij gerubriceerde werkzaamheden betrokken zijn of toegang hebben tot beveiligde communicatie- of informatiesystemen, te kennen en incidenten of manifeste zwakke plekken die op de veiligheid van invloed kunnen zijn, te registreren en te rapporteren.

6.5. **Veiligheidsstatus van het personeel**

Er worden procedures ingesteld om ervoor te zorgen dat, wanneer over een persoon negatieve informatie bekend wordt, wordt nagegaan of hij of zij betrokken is bij gerubriceerde werkzaamheden of toegang heeft tot beveiligde communicatie- of informatiesystemen, en dat ►M2 het directoraat Veiligheid van de Commissie ◄ wordt ingelicht. Als wordt geconstateerd dat genoemde persoon een veiligheidsrisico met zich meebrengt, wordt hij of zij uitgesloten of verwijderd van taken waar hij of zij de veiligheid in gevaar zou kunnen brengen.

▼B

7. FYSIEKE BEVEILIGING

7.1. **De noodzaak van bescherming**

De fysieke beveiligingsmaatregelen die worden toegepast om de bescherming van gerubriceerde EU-gegevens te waarborgen, moeten in verhouding staan tot het rubriceringsniveau, de omvang van en de bedreiging voor de aanwezige gegevens en het aanwezige materiaal. Alle houders van gerubriceerde EU-gegevens moeten voor de rubricering van die gegevens uniforme praktijken volgen en voldoen aan gemeenschappelijke normen voor de bescherming wat betreft bewaring, overdracht en verwijdering van te beschermen gegevens en materiaal.

7.2. **Controle**

Alvorens zones die gerubriceerde EU-gegevens bevatten onbemand achter te laten, moeten personen die met de bewaring zijn belast, ervoor zorgen dat de gegevens veilig zijn opgeborgen en dat alle beveiligingsmiddelen (sloten, alarm enz.) geactiveerd zijn. Ook na afloop van de werktijden worden onafhankelijke controles uitgevoerd.

7.3. **Beveiliging van gebouwen**

Gebouwen waarin gerubriceerde EU-gegevens of beveiligde communicatie- en informatiesystemen zijn gehuisvest, moeten tegen ongeoorloofde toegang worden beschermd. De aard van de bescherming die voor de gerubriceerde EU-gegevens wordt gebruikt, zoals bijvoorbeeld tralies voor vensters, deursloten, bewakers bij de ingangen, automatische toegangscontrolesystemen, beveiligingscontroles en -patrouilles, alarmsystemen, indringerdetectiesystemen en waakhonden hangt af van:

a) rubricering, volume en locatie binnen het gebouw, van te beschermen gegevens en materiaal;

b) de kwaliteit van de beveiligingsopbergmiddelen voor gegevens en materiaal; en

c) de fysieke aard en locatie van het gebouw.

De aard van de bescherming voor communicatie- en informatiesystemen is m.m. afhankelijk van de beoordeling van de waarde van deze systemen en de potentiële schade als zij gecompromitteerd worden, de fysieke aard en locatie van het gebouw waarin het systeem is gehuisvest en de locatie van het systeem binnen het gebouw.

7.4. **Calamiteitenplannen**

Er worden vooraf gedetailleerde plannen opgesteld voor de bescherming van gerubriceerde gegevens in plaatselijke of nationale noodsituaties.

8. INFORMATIEBEVEILIGING

Informatiebeveiliging (Infosec) heeft betrekking op de keuze en de toepassing van beveiligingsmaatregelen die gerubriceerde EU-gegevens die in communicatie-, informatie- en andere elektronische systemen worden verwerkt, opgeslagen of overgedragen, moeten beschermen tegen accidenteel of met opzet veroorzaakt verlies van het vertrouwelijke karakter, de integriteit of de beschikbaarheid ervan. Er moeten passende tegenmaatregelen worden genomen om te voorkomen dat niet-gemachtigde gebruikers toegang krijgen tot gerubriceerde EU-gegevens of dat gemachtigde gebruikers de toegang tot gerubriceerde EU-gegevens onmogelijk wordt gemaakt, en om te zorgen dat corruptie, ongeoorloofde wijziging of verwijdering van gerubriceerde EU-gegevens wordt voorkomen.

▼B

9. BEVEILIGING TEGEN SABOTAGE EN BESTRIJDING VAN ANDERE VORMEN VAN KWAADWILLIGE BESCHADIGING

Fysieke voorzorgen voor de bescherming van belangrijke installaties waarin zich gerubriceerde gegevens bevinden, bieden als veiligheidsmaatregel de beste bescherming tegen sabotage en kwaadwillige beschadiging; het veiligheidsonderzoek van het personeel alleen is daarvoor geen afdoend vervangmiddel. De bevoegde nationale instantie wordt verzocht inlichtingen te verstrekken over spionage, sabotage, terrorisme en andere subversieve activiteiten.

10. VRIJGAVE VAN GERUBRICEERDE GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES

Het besluit om van de Commissie afkomstige gerubriceerde EU-gegevens vrij te geven aan een derde staat of een internationale organisatie wordt door de Commissie als college genomen. Als de Commissie niet de opsteller is van de gegevens waarvan de vrijgave wordt gewenst, vraagt de Commissie vóór vrijgave toestemming aan de opsteller. Als niet kan worden achterhaald wie de opsteller is, neemt de Commissie de verantwoordelijkheid van de opsteller over.

Wanneer de Commissie van derde staten, internationale organisaties of andere derden gerubriceerde gegevens ontvangt, krijgen deze gegevens de bescherming die past bij de rubricering en overeenkomt met de normen die in de onderhavige veiligheidsvoorschriften voor gerubriceerde EU-gegevens worden vastgesteld, of met strengere normen als de derde die de gegevens vrijgeeft, daarom vraagt. Er kan een regeling worden getroffen voor wederzijdse controle.

Bovenstaande beginselen worden uitgevoerd overeenkomstig de bepalingen van deel II, afdeling 26, en de aanhangsels 3, 4 en 5.

DEEL II: ORGANISATIE VAN DE BEVEILIGING IN DE COMMISSIE

11. HET VOOR VEILIGHEID BEVOEGDE COMMISSIELID

Het voor veiligheid bevoegde Commissielid:

a) voert het veiligheidsbeleid van de Commissie uit;

b) bestudeert de veiligheidsproblemen die de Commissie of de onder haar ressorterende bevoegde instanties hem of haar voorleggen;

c) onderzoekt in nauwe samenwerking met de nationale veiligheidsinstanties (of andere relevante instanties) van de lidstaten (hierna NSA genoemd) vraagstukken die veranderingen in het veiligheidsbeleid van de Commissie met zich meebrengen.

Het voor veiligheid bevoegde Commissielid is meer bepaald verantwoordelijk voor:

a) de coördinatie van alle veiligheidskwesties die verband houden met de werkzaamheden van de Commissie;

b) het richten van verzoeken tot de daartoe aangewezen instanties van de lidstaten om de NSA overeenkomstig afdeling 20 beveiligingsmachtigingen te laten verstrekken voor personeel dat bij de Commissie werkzaam is;

c) het onderzoeken of laten onderzoeken van lekken van gerubriceerde EU-gegevens die zich, tot bewijs van het tegendeel, bij de Commissie hebben voorgedaan;

d) het richten van een verzoek tot de betrokken veiligheidsinstanties om een onderzoek in te leiden wanneer er buiten de Commissie gerubriceerde EU-gegevens uitgelekt zijn, en het coördineren van de onderzoeken wanneer er verschillende veiligheidsinstanties bij zijn betrokken;

e) het periodiek onderzoeken van beveiligingsregelingen voor de bescherming van gerubriceerde EU-gegevens;

▼B

f) het onderhouden van nauwe contacten met alle betrokken veiligheidsinstanties om te komen tot een volledige coördinatie op het gebied van de veiligheid;

g) het voortdurend in het oog houden van het beleid en de procedures van de Commissie inzake veiligheid en, zo nodig, het doen van passende aanbevelingen. Daartoe legt het voor veiligheid bevoegde Commissielid het door ►M2 het directoraat Veiligheid van de Commissie ◄ opgestelde jaarlijkse inspectieplan aan de Commissie voor.

12. DE ADVIESGROEP VEILIGHEIDSBELEID VAN DE COMMISSIE

Er wordt een Adviesgroep Veiligheidsbeleid van de Commissie opgericht, die bestaat uit het voor veiligheid bevoegde Commissielid of zijn afgevaardigde, die het voorzitterschap waarneemt, en uit vertegenwoordigers van de NSA van elke lidstaat. Er kunnen ook vertegenwoordigers van andere Europese instellingen worden uitgenodigd. Voorts kunnen vertegenwoordigers van relevante gedecentraliseerde EG- en EU-instanties worden uitgenodigd wanneer er aangelegenheden worden besproken die hen aanbelangen.

De Adviesgroep Veiligheidsbeleid van de Commissie komt bijeeen op verzoek van de voorzitter of een van haar leden. De opdracht van de groep bestaat erin alle relevante veiligheidskwesties te onderzoeken en te evalueren, en zo nodig aanbevelingen te doen aan de Commissie.

▼M2

13. DE ADVIESRAAD VEILIGHEID VAN DE COMMISSIE

Er wordt een Adviesraad Veiligheid van de Commissie opgericht bestaande uit de directeur-generaal voor Personeelszaken en administratie die het voorzitterschap waarneemt, een lid van het kabinet van het voor veiligheid bevoegde Commissielid, een lid van het kabinet van de Voorzitter, de adjunct-secretaris-generaal die het voorzitterschap van de groep voor crisisbeheer van de Commissie waarneemt, de directeuren-generaal van de Juridische dienst, Buitenlandse betrekkingen, Justitie, vrijheid en veiligheid, het Gemeenschappelijk Centrum voor onderzoek, Informatica en de dienst Interne audit, en de directeur van het directoraat Veiligheid van de Commissie, of hun vertegenwoordigers. Er kunnen ook andere ambtenaren van de Commissie worden uitgenodigd. De opdracht van deze adviesraad bestaat erin de veiligheidsmaatregelen in de Commissie te evalueren en terzake aanbevelingen te doen aan het voor veiligheid bevoegde Commissielid.

▼B

14. ►M2 HET DIRECTORAAT VEILIGHEID VAN DE COMMISSIE ◄

Met het oog op de uitoefening van zijn in afdeling 11 vermelde verantwoordelijkheden kan het voor veiligheid bevoegde Commissielid een beroep doen op ►M2 het directoraat Veiligheid van de Commissie ◄ voor het coördineren van, toezicht houden op en uitvoeren van de veiligheidsmaatregelen.

►M2 De directeur van het directoraat Veiligheid van de Commissie ◄ is de belangrijkste adviseur van het voor veiligheid bevoegde Commissielid; hij treedt op als secretaris van de Adviesgroep Veiligheidsbeleid. In dit verband leidt hij de actualisering van de veiligheidsvoorschriften en coördineert hij de veiligheidsmaatregelen met de bevoegde instanties van de lidstaten en, indien van toepassing, de internationale organisaties waarmee de Commissie veiligheidsovereenkomsten heeft gesloten. Met het oog daarop treedt hij op als verbindingsambtenaar.

►M2 De directeur van het directoraat Veiligheid van de Commissie ◄ is verantwoordelijk voor de accreditatie van IT-systemen en -netwerken in de Commissie en besluit, in overleg met de betrokken NSA, over de accreditatie van IT-systemen en -netwerken waarbij enerzijds de Commissie en anderzijds andere ontvangers van gerubriceerde EU-gegevens zijn betrokken.

▼B

15. VEILIGHEIDSINSPECTIES

►M2 Het directoraat Veiligheid van de Commissie ◄ verricht periodieke inspecties van de beveiligingsregelingen voor de bescherming van gerubriceerde EU-gegevens.

►M2 Het directoraat Veiligheid van de Commissie ◄ kan bij deze taak worden bijgestaan door de veiligheidsdiensten van andere EU-instellingen die EUCI in hun bezit hebben, of door de nationale veiligheidsinstanties van de lidstaten [1].

Op verzoek van een lidstaat kan de NSA van die lidstaat, samen met ►M2 het directoraat Veiligheid van de Commissie ◄ en met wederzijdse instemming, binnen de Commissie inspecties van EUCI verrichten.

16. RUBRICERINGEN, BEVEILIGINGSINDICATOREN EN MARKERINGEN

16.1. **Rubriceringsniveaus** [2]

De volgende rubriceringsniveaus worden gehanteerd (zie ook aanhangsel 2):

►M1 TRES SECRET UE/EU TOP SECRET ◄: deze rubricering wordt alleen toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging uitzonderlijk nadelig zou kunnen zijn voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten.

►M1 SECRET UE ◄: deze rubricering wordt alleen toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging ernstige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten.

►M1 CONFIDENTIEL UE ◄: deze rubricering wordt toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten.

►M1 RESTREINT UE ◄: deze rubricering wordt toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelig zou kunnen zijn voor de belangen van de Europese Unie of van één of meer van haar lidstaten.

Andere rubriceringen zijn niet toegestaan.

16.2. **Beveiligingsindicator**

Om de geldigheidsduur van een rubricering te beperken (wat voor gerubriceerde gegevens inhoudt dat zij automatisch lager worden gerubriceerd of worden gederubriceerd) kan een overeengekomen beveiligingsindicator worden gebruikt. Deze indicator is „TOT… (uur/datum)” of „TOT… (feit)”.

Zijn een beperkte verspreiding en een bijzondere verwerking nodig (ter aanvulling van die op grond van de rubricering), dan worden extra beveiligingsindicatoren gebruikt, zoals Crypto of andere door de EU erkende beveiligingsindicatoren.

Beveiligingsindicatoren mogen alleen worden gebruikt in combinatie met een rubricering.

16.3. **Markeringen**

Er kan een markering worden gebruikt waarmee het volgende wordt aangegeven: het domein waarop het document betrekking heeft, een speciale verspreiding op „need to know”-basis of, voor niet-gerubriceerde gegevens, het einde van een publicatieverbod.

Een markering is geen rubricering en mag niet in plaats daarvan worden gebruikt.

([1]) Onverminderd het Verdrag van Wenen inzake diplomatiek verkeer van 1961 en het Protocol betreffende de voorrechten en immuniteiten van de Europese Gemeenschappen van 8 april 1965.

([2]) Aanhangsel 1 bevat een vergelijkend overzicht van de beveiligingsniveaus van EU, NAVO, WEU en de lidstaten.

▼B

De markering ESDP wordt aangebracht op documenten en kopieën daarvan die betrekking hebben op de veiligheid en defensie van de Europese Unie of van één of meer van haar lidstaten, of die betrekking hebben op militair of niet-militair crisisbeheer.

16.4. **Aanbrengen van een rubricering**

De rubricering zal als volgt worden aangebracht:

a) op ►M1 RESTREINT UE ◄-documenten, met mechanische of elektronische middelen,

b) op ►M1 CONFIDENTIEL UE ◄-documenten, met mechanische middelen en met de hand of door het drukken op voorgemerkt, geregistreerd papier,

c) op ►M1 SECRET UE ◄- en ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten, met mechanische middelen en met de hand.

16.5. **Aanbrengen van beveiligingsindicatoren**

De beveiligingsindicatoren worden onmiddellijk onder de rubricering aangebracht, met dezelfde middelen als die waarmee de rubricering is aangebracht.

17. RUBRICERINGSBEHEER

17.1. **Algemeen**

Gegevens worden alleen gerubriceerd wanneer dat noodzakelijk is. De rubricering moet duidelijk en correct worden aangegeven en mag slechts gehandhaafd worden zolang de gegevens beschermd moeten worden.

De verantwoordelijkheid voor het rubriceren van de gegevens en een eventuele lagere rubricering of derubricering berust uitsluitend bij de bron.

Rubricering, lagere rubricering of derubricering worden uitgevoerd door ambtenaren of andere personeelsleden van de Commissie, volgens de instructies of met de instemming van het hoofd van de dienst.

De gedetailleerde procedures voor de behandeling van gerubriceerde documenten moeten zo zijn opgezet dat een aan de inhoud aangepaste bescherming is gegarandeerd.

Het aantal personen dat gemachtigd is om ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten op te stellen wordt tot een minimum beperkt, en hun namen worden op een lijst geplaatst die door het Veiligheidsbureau wordt bijgehouden.

17.2. **Rubricering**

De rubriceringsgraad van een document wordt bepaald naar gelang van het niveau van gevoeligheid van de inhoud, overeenkomstig de definities die in afdeling 16 zijn gegeven. Het is van belang dat op correcte en zuinige wijze met rubricering wordt omgesprongen. Dit geldt in het bijzonder voor de rubriceringsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄.

De opsteller van een te rubriceren document moet rekening houden met de hierboven bedoelde voorschriften en moet over- of onderrubricering vermijden.

In aanhangsel 2 is een praktische rubriceringsgids opgenomen.

Afzonderlijke bladzijden, punten, afdelingen, bijlagen, aanhangsels, aanhechtsels en bijvoegsels van een bepaald document kunnen verschillende rubriceringen vereisen en moeten dienovereenkomstig gemarkeerd worden. De rubricering die voor het gehele document geldt, is in dat geval die van het hoogst gerubriceerde gedeelte.

▼B

De rubricering van een brief of een nota die bijvoegsels vergezelt is van dezelfde graad als het hoogst gerubriceerde bijvoegsel. Aan de bron dient duidelijk te worden aangegeven welke rubricering op die brief of nota moet worden toegepast indien deze gescheiden wordt van de bijvoegsels.

Voor de toegang van het publiek tot de documenten, blijft Verordening (EG) nr. 1049/2001 van toepassing.

17.3. **Lagere rubricering en derubricering**

Gerubriceerde EU-documenten kunnen alleen lager gerubriceerd of gederubriceerd worden met de toestemming van de opsteller en, zonodig, na bespreking met de betrokken partijen. Lagere rubricering en derubricering moeten schriftelijk bevestigd worden. De opsteller van het document is er verantwoordelijk voor dat de geadresseerden van de wijziging op de hoogte worden gebracht; deze geadresseerden zijn er op hun beurt verantwoordelijk voor dat de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het gekopieerd hebben, van de wijziging op de hoogte worden gebracht.

Zo mogelijk vermelden de opstellers op gerubriceerde documenten een datum waarop of een periode waarna de inhoud lager gerubriceerd of gederubriceerd kan worden. Zo niet verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkelijke rubricering moet worden gehandhaafd.

18. FYSIEKE BEVEILIGING

18.1. **Algemeen**

De belangrijkste doelstelling van de fysieke beveiligingsmaatregelen bestaat erin te verhinderen dat een niet-gemachtigde persoon toegang krijgt tot gerubriceerde EU-gegevens en/of gerubriceerd EU-materiaal, te voorkomen dat materieel of andere eigendommen worden gestolen of beschadigd, en ervoor te zorgen dat zich geen ongewenste intimiteiten of enige andere vorm van agressie voordoen onder ambtenaren, andere werknemers of bezoekers.

18.2. **Veiligheidseisen**

Alle gebouwen, zones, ruimten, bureaus, communicatie- en informatiesystemen, enz., waar gerubriceerde EU-gegevens en gerubriceerd EU-materiaal worden bewaard en/of verwerkt, moeten met passende fysieke beveiligingsmaatregelen worden beschermd.

Om te bepalen in welke mate bescherming met fysieke beveiligingsmaatregelen noodzakelijk is, worden alle relevante factoren in aanmerking genomen, zoals:

a) de rubriceringsgraad van de gegevens en/of het materiaal;

b) de hoeveelheid en de vorm (bijvoorbeeld niet-elektronisch document, digitaal opslagmedium) van de gegevens;

c) de plaatselijk beoordeelde bedreiging die uitgaat van inlichtingendiensten die zich toeleggen op de EU, de lidstaten en/of instellingen of derde partijen die gerubriceerde EU-gegevens bewaren, met name in de vorm van sabotage, terrorisme of andere subversieve en/of criminele activiteiten.

Met de fysieke beveiligingsmaatregelen wordt beoogd:

a) het binnendringen met list of geweld te verhinderen;

b) acties van malafide personeelsleden te ontmoedigen, te verhinderen en op te sporen;

c) de toegang tot gerubriceerde EU-gegevens te ontzeggen aan personen die niet beantwoorden aan het „need-to-know”-criterium.

▼B

18.3. **Fysieke beveiligingsmaatregelen**

18.3.1. *Veiligheidszones*

Zones waar als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens worden verwerkt en opgeslagen worden zodanig opgezet en gestructureerd dat zij aan de onderstaande voorwaarden voldoen:

a) Veiligheidszone van klasse I: een zone waar als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens zodanig worden verwerkt en opgeslagen dat toegang tot de zone in de praktijk neerkomt op toegang tot gerubriceerde gegevens. Voor een dergelijke zone is het volgende vereist:

   i) een duidelijk omschreven, beschermde afscheiding waar elk in- en uitgaan wordt gecontroleerd,

   ii) een zodanig toegangscontrolesysteem dat uitsluitend diegenen die naar behoren zijn gescreend en speciaal gemachtigd zijn, de zone kunnen betreden,

   iii) specificatie van de rubriceringsgraad van de gegevens die normaliter in de zone worden bewaard, dat wil zeggen van de gegevens waartoe men na binnenkomst toegang heeft;

b) Veiligheidszone van klasse II: een zone waar als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens zodanig worden verwerkt en opgeslagen dat zij tegen toegang door niet gemachtigden kan worden beschermd via intern opgezette controles, bijvoorbeeld een ruimte waar kantoren zijn ondergebracht waar als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens regelmatig worden verwerkt en opgeslagen. Voor een dergelijke zone is het volgende vereist:

   i) een duidelijk omschreven, beschermde afscheiding waar elk in- en uitgaan wordt gecontroleerd,

   ii) een zodanig toegangscontrolesysteem dat uitsluitend diegene, die naar behoren zijn gescreend en speciaal gemachtigd zijn, de zone onbegeleid kunnen betreden. Voor alle andere personen zal worden voorzien in begeleiding of gelijkwaardige controles, om te voorkomen dat niet-gemachtigden toegang krijgen tot gerubriceerde EU-gegevens, en dat zonder controle zones kunnen worden betreden die zijn onderworpen aan technische veiligheidsinspecties.

   Zones waar niet op 24-uursbasis personeel aanwezig is, worden onmiddellijk na de normale werkuren geïnspecteerd, om na te gaan of de gerubriceerde EU-gegevens veilig zijn weggeborgen.

18.3.2. *Administratieve zone*

Nabij of vóór de veiligheidszones van klasse I of klasse II kan een administratieve zone met een lager veiligheidsniveau worden geïnstalleerd. Voor een dergelijke zone is een duidelijk omschreven afscheiding nodig, waar personeel en voertuigen kunnen worden gecontroleerd. Binnen administratieve zones kunnen alleen als ►M1 RESTREINT UE ◄ gerubriceerde gegevens en niet-gerubriceerde gegevens worden verwerkt en opgeslagen.

18.3.3. *Controles bij in- en uitgaan*

Het betreden van veiligheidszones van klasse I en klasse II wordt gecontroleerd aan de hand van een pasje of een persoonsherkenningssysteem voor het vaste personeel. Tevens moet een controlesysteem voor bezoekers worden opgezet om de toegang tot gerubriceerde EU-gegevens door niet-gemachtigden te verhinderen. Het pasjessysteem kan worden ondersteund door geautomatiseerde identificatie, die moet worden beschouwd als een aanvulling op, maar niet geheel in de plaats mag komen van, bewakers. Een wijziging in de dreigingsbeoordeling kan een versterking meebrengen van de maatregelen op het gebied van controle bij in- en uitgaan, bijv. tijdens het bezoek van prominenten.

▼B

18.3.4. *Bewakingspatrouilles*

Buiten de normale werkuren moet in de veiligheidszones van klasse I en klasse II worden gepatrouilleerd om EU-materiaal te beschermen tegen compromittering, beschadiging of verlies. De frequentie waarmee wordt gepatrouilleerd wordt bepaald naar gelang van de plaatselijke omstandigheden; een vuistregel is echter om de twee uur te patrouilleren.

18.3.5. *Beveiligingsopbergmiddelen en braakwerende ruimten*

Voor de opslag van gerubriceerde EU-gegevens worden drie klassen opbergmiddelen gebruikt:

— klasse A: opbergmiddelen die op nationaal niveau zijn goedgekeurd voor de opslag van als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens in veiligheidszones van klasse I of klasse II;

— klasse B: opbergmiddelen die op nationaal niveau zijn goedgekeurd voor de opslag van als ►M1 SECRET UE ◄ en ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens in veiligheidszones van klasse I of klasse II;

— klasse C: kantoormeubilair dat zich uitsluitend leent voor de opslag van als ►M1 RESTREINT UE ◄ gerubriceerde gegevens.

In braakwerende ruimten die zijn ingericht binnen een veiligheidszone van klasse I of klasse II, en voor alle veiligheidszones van klasse I waar als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens in rekken zijn opgeslagen of kunnen worden afgelezen van grafieken, kaarten, enz., moeten muren, vloeren en plafonds, en deuren met sloten door een nationale veiligheidsinstantie (NSA) worden gecertificeerd als zijnde van een gelijkwaardig beschermingsniveau als de klasse beveiligingsopbergmiddelen die zijn goedgekeurd voor de opslag van gegevens met dezelfde rubricering.

18.3.6. *Sloten*

Sloten op beveiligingsopbergmiddelen en braakwerende ruimten waarin gerubriceerde EU-gegevens zijn opgeslagen, moeten aan de volgende normen voldoen:

— groep A: op nationaal niveau goedgekeurd voor opbergmiddelen van klasse A;

— groep B: op nationaal niveau goedgekeurd voor opbergmiddelen van klasse B;

— groep C: alleen geschikt voor kantoormeubilair van klasse C.

18.3.7. *Controle van sleutels en codecombinaties*

Sleutels van beveiligde opbergmiddelen mogen niet worden meegenomen buiten het gebouw. Codecombinaties van beveiligingsopbergmiddelen moeten worden gememoriseerd door personen die hiervan kennis moeten nemen. De veiligheidsambtenaar van de betrokken dienst bewaart reservesleutels en een overzicht op papier van alle codecombinatie, voor gebruik in noodgevallen; dit overzicht wordt in afzonderlijke verzegelde ondoorzichtige enveloppen bewaard. De gewone sleutel, de extra beveiligingssleutels en de codecombinaties worden in afzonderlijke beveiligingsopbergmiddelen bewaard. Sleutels en codecombinaties krijgen ten minste hetzelfde beschermingsniveau als het materiaal waartoe zij toegang verschaffen.

Zo weinig mogelijk mensen mogen de codecombinaties van beveiligingsopbergmiddelen kennen. De combinaties worden gewijzigd:

a) bij ontvangst van nieuwe opbergmiddelen;

b) bij wijzigingen in de personeelsbezetting;

c) wanneer compromittering heeft plaatsgevonden of wordt vermoed;

d) met tussenpozen van bij voorkeur zes maanden, maar in ieder geval om de twaalf maanden.

▼B

18.3.8. *Indringerdetectie-/signaleringssystemen*

Wanneer voor de bescherming van gerubriceerde EU-gegevens alarmsystemen, een gesloten televisiecircuit of andere elektrische systemen worden gebruikt, dient er een noodaggregaat beschikbaar te zijn om de continuwerking van het systeem te waarborgen wanneer de hoofdelektriciteitsvoorziening uitvalt. Een andere fundamentele vereiste is dat er een alarmsignaal of een andere betrouwbare waarschuwing uitgaat naar het bewakingspersoneel als dergelijke systemen slecht functioneren of gepoogd wordt ze te saboteren.

18.3.9. *Goedgekeurde uitrusting*

Het Veiligheidbureau houdt bijgewerkte lijsten bij, per type en model, van de beveiligingsuitrusting die zij hebben goedgekeurd voor de bescherming van gerubriceerde gegevens onder diverse gespecificeerde omstandigheden en voorwaarden. Deze lijsten zijn onder meer gebaseerd op informatie van de NSA's.

18.3.10. *Fysieke bescherming van kopieermachines en faxapparaten*

Kopieermachines en faxapparaten moeten zodanig fysiek worden beschermd dat zij voor de verwerking van gerubriceerde gegevens alleen door gemachtigde personen kunnen worden gebruikt, en dat alle gerubriceerde producten op passende wijze worden gecontroleerd.

18.4. **Bescherming tegen waarneming van buitenaf en afluisteren**

18.4.1. *Waarneming van buitenaf*

Overdag en 's nachts dienen alle passende maatregelen te worden genomen om ervoor te zorgen dat gerubriceerde EU-gegevens niet door onbevoegden kunnen worden waargenomen, zelfs niet per ongeluk.

18.4.2. *Afluisteren*

Kantoren of zones waar regelmatig als ►**M1** SECRET UE ◄ en hoger gerubriceerde gegevens worden besproken, moeten worden beschermd tegen passief en actief afluisteren wanneer het risico dit vereist. De risicoanalyse van dergelijke incidenten behoort tot de verantwoordelijkheid van de bevoegde veiligheidsinstantie, indien nodig na overleg met de NSA's.

18.4.3. *Binnenbrengen van elektronische registratieapparatuur*

Het is niet toegelaten mobiele telefoons, privé-computers, opnameapparatuur, camera's of andere elektronische registratieapparatuur in veiligheidszones of in technisch veilige zones binnen te brengen zonder de voorafgaande toestemming van het hoofd van het Veiligheidsbureau.

Bij het bepalen van de beschermende maatregelen die moeten worden genomen in ruimten die gevoelig zijn voor passief afluisteren (bv. isoleren van muren, deuren, vloeren en plafonds, meting van compromitterende geluiden) en actief afluisteren (bv. het zoeken naar microfoons), kan ►**M2** de directeur van het directoraat Veiligheid van de Commissie ◄ om bijstand van deskundigen NSA's verzoeken.

Ook de telecommunicatie-installatie en de elektrische of elektronische bureau-uitrusting van ongeacht welk type dat gedurende bijeenkomsten van het niveau ►**M1** SECRET UE ◄ en hoger wordt gebruikt, kunnen op verzoek van de bevoegde beveiligingsfunctionaris door technische-beveiligingsspecialisten van NSA's worden gecontroleerd wanneer de omstandigheden zulks vereisen.

▼B

18.5. **Technisch veilige zones**

Bepaalde zones kunnen als „technisch veilig" worden aangewezen. Hier wordt een speciale toegangscontrole uitgevoerd. Dergelijke zones worden via een goedgekeurde methode afgesloten wanneer zij niet in gebruik zijn, en alle sleutels worden als veiligheidssleutels behandeld. Dergelijke zones worden onderworpen aan regelmatige fysieke inspecties, ook nadat zij zijn betreden door een niet-gemachtigde persoon of wanneer daarvan het vermoeden bestaat.

Voor controledoeleinden zal een uitvoerige lijst van installaties en meubilair worden bijgehouden. Meubelstukken of apparatuur mogen niet in een dergelijke zone worden binnengebracht zolang zij niet door speciaal opgeleid veiligheidspersoneel aan een zorgvuldige inspectie zijn onderworpen om mogelijke afluisterapparatuur op te sporen. Als algemene regel geldt dat in technisch veilige zones geen communicatielijnen mogen worden geïnstalleerd zonder voorafgaande machtiging door de bevoegde instantie.

19. ALGEMENE VOORSCHRIFTEN BETREFFENDE HET NEED-TO-KNOW-BEGINSEL EN HET VEILIGHEIDSONDERZOEK

19.1. **Algemeen**

Toegang tot gerubriceerde EU-gegevens mag slechts worden verleend aan personen die een „need-to-know" hebben, d.w.z. personen die in verband met de uitvoering van hun opdrachten of missies kennis moeten nemen van gerubriceerde EU-gegevens. Toegang tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens mag alleen worden verleend aan personen die in het bezit zijn van een passende veiligheidsmachtiging.

De verantwoordelijkheid om te bepalen wie een „need-to-know" heeft, berust bij de afdeling waar de betrokkene in dienst zal worden genomen.

De verantwoordelijkheid voor het veiligheidsonderzoek van het personeel berust bij de betrokken afdeling.

Dit resulteert in de afgifte van een „veiligheidsattest", waarop de rubriceringsgraad is vermeld waartoe de gemachtigde toegang heeft, alsook de datum waarop deze machtiging verstrijkt.

Een veiligheidsmachtiging voor een bepaalde rubricering kan de houder toegang verlenen tot informatie van een lagere rubriceringsgraad.

Niet-personeelsleden — bijvoorbeeld externe contractanten, deskundigen of consulenten — met wie noodzakelijkerwijs gerubriceerde EU-gegevens moeten worden besproken, of aan wie deze moeten worden getoond, moeten over een veiligheidsmachtiging voor gerubriceerde EU-gegevens beschikken en moeten instructies krijgen omtrent hun verantwoordelijkheid vanuit veiligheidsoogpunt.

Voor de toegang van het publiek tot de documenten, blijft Verordening (EG) nr. 1049/2001 van toepassing.

19.2. **Specifieke voorschriften inzake de toegang tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens**

Iedereen die toegang moet krijgen tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens, moet eerst een veiligheidsonderzoek ondergaan.

De personen die toegang moeten krijgen tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens, worden aangewezen door het Commissielid dat bevoegd is voor veiligheidsaangelegenheden; hun naam wordt opgenomen in een speciaal „►M1 TRES SECRET UE/EU TOP SECRET ◄-register".

▼B

Iedereen die toegang moet krijgen tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens, moet eerst een attest ondertekenen waarin hij/zij verklaart kennis te hebben genomen van de bij de Commissie geldende procedures inzake beveiliging en zich ten volle bewust te zijn van de bijzondere verantwoordelijkheid die op hem/haar rust om geheimhouding omtrent de als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens te waarborgen, alsook van de gevolgen die krachtens de voorschriften van de EU en de nationale wettelijke of bestuursrechtelijke bepalingen zijn verbonden aan het met opzet of door nalatigheid doorgeven van gerubriceerde gegevens aan onbevoegden.

Wanneer iemand tijdens een vergadering toegang krijgt tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens, moet de bevoegde controleambtenaar van de dienst of de instantie waarbij de betrokkene in dienst is, de instantie die de vergadering organiseert ervan in kennis stellen dat deze persoon hiertoe gemachtigd is.

De namen van diegenen die niet langer belast zijn met taken waarvoor toegang tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens vereist is, worden verwijderd uit het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register. Daarbij wordt nogmaals gewezen op de bijzondere verantwoordelijkheid die op hen rust om geheimhouding omtrent de als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens te waarborgen. Tevens dienen zij een verklaring te ondertekenen dat zij de als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens die in hun bezit zijn, niet zullen gebruiken of doorgeven.

19.3. **Specifieke voorschriften inzake de toegang tot als ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens**

Alle personen die toegang hebben tot als ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens, worden eerst aan een veiligheidsonderzoek voor het passende niveau onderworpen.

Alle personen die toegang hebben tot als ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens moeten in kennis worden gesteld van de ter zake strekkende veiligheidsvoorschriften en moeten zich bewust zijn van de gevolgen van nalatigheid.

Wanneer iemand tijdens een vergadering toegang krijgt tot als ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens, moet de bevoegde controleambtenaar van de dienst of de instantie waarbij de betrokkene in dienst is, de instantie die de vergadering organiseert ervan in kennis stellen dat deze persoon hiertoe gemachtigd is.

19.4. **Specifieke voorschriften inzake de toegang tot als ►M1 RESTREINT UE ◄ gerubriceerde gegevens**

Personen die toegang hebben tot als ►M1 RESTREINT UE ◄ gerubriceerde gegevens moeten in kennis worden gesteld van de ter zake strekkende veiligheidsvoorschriften en van de gevolgen van nalatigheid.

19.5. **Overdracht**

Wanneer een personeelslid een ambt verlaat dat de verwerking van gerubriceerd EU-materiaal impliceert, ziet het Register erop toe dat dit materiaal op correcte wijze door de vertrekkende ambtenaar aan zijn opvolger wordt overgedragen.

Wanneer een personeelslid wordt overgeplaatst naar een ambt dat de verwerking van gerubriceerd EU-materiaal impliceert, krijgt het de nodige instructies van de plaatselijke veiligheidsambtenaar.

19.6. **Speciale instructies**

Personen die met de verwerking van gerubriceerde EU-gegevens worden belast, moeten bij het aanvaarden van hun functie en vervolgens op gezette tijden instructies krijgen betreffende:

a) de veiligheidsrisico's die het gevolg zijn van loslippigheid;

b) de voorzorgen die zij moeten nemen bij hun contacten met de pers en met vertegenwoordigers van belangengroepen;

▼B

c) de dreiging die uitgaat van de activiteiten van inlichtingendiensten die de EU en de lidstaten als doelwit zien wat betreft gerubriceerde EU-gegevens en -activiteiten;

d) de verplichting bij de relevante veiligheidsinstanties onmiddellijk verslag uit te brengen van elke bejegening of handeling die aanleiding geeft tot een vermoeden van spionage, of van elke ongebruikelijke situatie op het stuk van de veiligheid.

Alle personen die normaliter veelvuldig contact hebben met vertegenwoordigers uit landen wier inlichtingendiensten de EU en lidstaten als doelwit zien voor wat betreft gerubriceerde EU-gegevens en -activiteiten, moeten instructies krijgen over de technieken waarvan bekend is dat zij door diverse inlichtingendiensten worden gebruikt.

Er bestaan bij de Commissie geen speciale veiligheidsmaatregelen voor privéreizen, naar welke bestemming ook, van personen die in het bezit zijn van een veiligheidsmachtiging voor toegang tot gerubriceerde EU-gegevens. Niettemin zal ►M2 het directoraat Veiligheid van de Commissie ◄ de ambtenaren en de andere personeelsleden die onder zijn verantwoordelijkheid vallen inlichten over de reisvoorschriften die voor hen van toepassing kunnen zijn.

20. PROCEDURE MET BETREKKING TOT HET VEILIGHEIDSONDERZOEK VOOR AMBTENAREN EN ANDERE PERSONEELSLEDEN VAN DE COMMISSIE

a) Alleen ambtenaren en andere personeelsleden van de Commissie en personen die voor de Commissie werken en die uit hoofde van hun functie en het belang van de dienst kennis moeten nemen of gebruik moeten maken van bij de Commissie bewaarde gerubriceerde gegevens, krijgen toegang tot deze gegevens.

b) Om toegang te krijgen tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens, moeten bovengenoemde personen gemachtigd zijn overeenkomstig de hierna beschreven procedure.

c) Machtiging wordt alleen verleend aan personen die aan een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten, (NSA's) zijn onderworpen overeenkomstig de in de punten i) tot en met n) bedoelde procedure.

d) Het hoofd van het Veiligheidsbureau is bevoegd om de bovengenoemde machtiging te verlenen.

e) Hij/zij verleent machtiging nadat het advies van de bevoegde nationale instanties van de lidstaten is ingewonnen, dat gebaseerd is op het veiligheidsonderzoek dat overeenkomstig de punten i) tot en met n) is uitgevoerd.

f) ►M2 Het directoraat Veiligheid van de Commissie ◄ houdt een bijgewerkte lijst van alle gevoelige functies bij op basis van de door de betrokken diensten van de Commissie verstrekte gegevens, alsmede een lijst van alle personen aan wie een (tijdelijke) machtiging is afgegeven.

g) De machtiging wordt verleend voor een periode van vijf jaar; zij blijft evenwel slechts geldig zolang de functie wordt vervuld op grond waarvan zij is verleend. Zij kan volgens de procedure van punt e) worden verlengd

h) Een machtiging kan door het hoofd van het Veiligheidsbureau worden ingetrokken, wanneer hij/zij meent dat daarvoor te rechtvaardigen gronden aanwezig zijn. Van ieder besluit tot intrekking van een machtiging wordt kennis gegeven aan de betrokkene gebracht, die kan verzoeken door het hoofd van het Veiligheidsbureau te worden gehoord, en aan de bevoegde nationale instantie.

▼B

i) Een veiligheidsonderzoek wordt, met de medewerking van de betrokkene en op verzoek van het hoofd van het Veiligheidsbureau, uitgevoerd door de bevoegde nationale instanties van de lidstaat waarvan de betrokkene onderdaan is. Wanneer de betrokkene geen onderdaan van een EU-lidstaat is, kan het hoofd van het Veiligheidsbureau de nationale instanties van de lidstaat waar de betrokkene zijn woonplaats heeft of geregeld verblijf houdt, verzoeken een veiligheidsonderzoek uit te voeren.

j) Een onderdeel van het veiligheidsonderzoek bestaat erin dat door de betrokkene een formulier met persoonlijke gegevens wordt ingevuld.

k) Het hoofd van het Veiligheidsbureau specificeert in zijn verzoek het type en het niveau van de gerubriceerde gegevens waartoe de betrokkene toegang moet krijgen, zodat de bevoegde nationale instanties het veiligheidsonderzoek kunnen uitvoeren, en hun advies kunnen geven rekening houdend met de machtigingsgraad die aan de betrokkene moet worden toegekend.

l) Voor de gehele procedure en de resultaten van het veiligheidsonderzoek gelden de in de betrokken lidstaat van toepassing zijnde voorschriften, ook wat de mogelijkheden tot beroep betreft.

m) Wanneer de bevoegde nationale instanties van de lidstaat een positief advies uitbrengen, kan ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄ de betrokkene machtiging verlenen.

n) Van een negatief advies van de bevoegde nationale instanties wordt kennis gegeven aan de betrokkene, die mag verzoeken te worden gehoord door ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄. Wanneer hij het nodig acht, kan ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄ de bevoegde nationale instanties vragen om, waar mogelijk, opheldering te verschaffen. Indien het negatief advies wordt bevestigd, wordt geen machtiging verleend.

o) Alle personen aan wie machtiging wordt verleend in de zin van de punten d) en e) ontvangen op het tijdstip dat de machtiging wordt verleend en vervolgens met regelmatige tussenpozen, alle noodzakelijke instructies betreffende de bescherming van gerubriceerde gegevens en de wijze waarop deze kan worden gewaarborgd. Zij ondertekenen een verklaring waarin zij erkennen de instructies te hebben ontvangen, en verbinden zich ertoe deze op te volgen.

p) ►M2 De directeur van het directoraat Veiligheid van de Commissie ◄ neemt alle noodzakelijke maatregelen tot uitvoering van deze afdeling, met name wat betreft de voorschriften die gelden voor de toegang tot de lijst van gemachtigden.

q) Bij wijze van uitzondering mag ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄ wanneer de dienst zulks vereist, nadat hij de nationale bevoegde instanties heeft geïnformeerd en mits deze niet binnen een maand reageren, in afwachting van het resultaat van het onderzoek waarnaar in punt i) wordt verwezen, tijdelijke machtiging verlenen voor een periode van hoogstens zes maanden.

r) De voorlopige en tijdelijke machtigingen die aldus worden verleend, geven geen toegang tot als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens; deze toegang blijft beperkt tot ambtenaren die daadwerkelijk, overeenkomstig punt i), met goed gevolg het veiligheidsonderzoek hebben ondergaan. Hangende het resultaat van dit onderzoek mag aan ambtenaren voor wie de machtigingsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄ is aangevraagd, tijdelijk en voorlopig machtiging worden verleend om toegang te hebben tot gegevens die gerubriceerd zijn tot en met de graad ►M1 SECRET UE ◄.

▼B

21. VERVAARDIGING, VERSPREIDING, OVERDRACHT, BEVEILIGING VAN KOERIERS, EXTRA KOPIEËN, VERTALINGEN EN UITTREKSEL VAN GERUBRICEERD EU-MATERIAAL

21.1. **Vervaardiging**

1. De EU-rubriceringen moeten overeenkomstig afdeling 16 worden toegepast; voor de rubriceringsgraden ►M1 CONFIDENTIEL UE ◄ en hoger moet de rubriceringsgraad op elke bladzijde midden bovenaan en midden onderaan worden aangebracht en moet elke bladzijde genummerd zijn. Op elk gerubriceerd EU-document moet een referentienummer en een datum voorkomen. Bij ►M1 TRES SECRET UE/EU TOP SECRET ◄- en ►M1 SECRET UE ◄-documenten wordt het referentienummer op elke bladzijde vermeld. Wanneer verschillende kopieën verspreid worden, moeten op de eerste bladzijde van elke kopie een kopienummer en het totaal aantal bladzijden vermeld zijn. Bij als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde documenten moet op de eerste bladzijde een lijst voorkomen van alle bijlagen en bijvoegsels.

2. Het typen, vertalen, opslaan, fotokopiëren, magnetisch reproduceren en op microfilm zetten van als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde documenten mag uitsluitend geschieden door personen die gemachtigd zijn voor toegang tot gerubriceerde EU-gegevens met minste de rubriceringsgraad van het betrokken document.

3. De voorschriften die gelden voor gerubriceerde documenten die met de computer worden verwerkt staan in afdeling 25.

21.2. **Verspreiding**

1. Gerubriceerde EU-gegevens mogen alleen verspreid worden onder personen met een „need-to-know” die over de desbetreffende veiligheidsmachtiging beschikken. De opsteller van het document specificeert de initiële verspreiding.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ documenten worden verspreid via de ►M1 TRES SECRET UE/EU TOP SECRET ◄-registers (zie afdeling 22.2). Wanneer het berichten met rubriceringsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄ betreft, kan het bevoegde register het hoofd van het communicatiecentrum machtigen om het aantal kopieën te maken dat in de lijst van de geadresseerden vermeld is.

3. Documenten met rubriceringsgraad ►M1 SECRET UE ◄ of lager mogen door de oorspronkelijke geadresseerde aan andere geadresseerden met een „need-to-know” worden doorgezonden. Als de instanties die het document hebben opgesteld echter beperkingen wensen op te leggen, moeten zij duidelijke waarschuwingsmarkeringen aanbrengen. In dat geval mag de geadresseerde de documenten alleen doorzenden met de toestemming van de instanties waarvan de documenten afkomstig zijn.

4. Documenten met rubriceringsgraad ►M1 CONFIDENTIEL UE ◄ worden bij aankomst in of vertrek uit een gebouw geregistreerd door het plaatselijk EUCI-Register. Daarbij worden bijzonderheden vermeld (referenties, datum en, in voorkomend geval, het kopienummer) waarmee de documenten kunnen worden geïdentificeerd; die gegevens worden in een logboek ingeschreven of in een speciaal beveiligd computermedium ingevoerd (zie afdeling 22.1).

21.3. **Overdracht van gerubriceerde EU-documenten**

21.3.1. *Verpakking, ontvangstbewijzen*

1. Als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde documenten worden in stevige, ondoorzichtige dubbele enveloppen vervoerd. Op de binnenste enveloppe wordt de toepasselijke EU-rubriceringsgraad aangebracht, alsmede voor zover mogelijk bijzonderheden zoals functie en adres van de ontvanger.

▼B

2. De binnenste enveloppe mag alleen worden geopend door een functionaris voor de registercontrole (zie 22.1) of door diens plaatsvervanger, die voor ontvangst van de ingesloten documenten tekent, behalve wanneer de enveloppe aan een welbepaalde persoon is geadresseerd. In dat geval (zie 22.1) wordt de aankomst van de enveloppe in het register genoteerd, en mag alleen de geadresseerde de binnenste enveloppe openen en voor ontvangst van de daarin ingesloten documenten tekenen.

3. In de binnenste enveloppe wordt een ontvangstbewijs ingesloten. Op dat bewijs, dat niet gerubriceerd wordt, moeten het referentienummer, de datum en het kopienummer van het document voorkomen; het onderwerp van het document mag echter nooit op het ontvangstbewijs worden vermeld.

4. De binnenste enveloppe wordt in een andere enveloppe gestoken, waarop een paknummer voor de ontvangstregistratie wordt aangebracht. De rubriceringsgraad mag in geen geval op de buitenste enveloppe voorkomen.

5. Voor als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde documenten krijgen koeriers en boodschappers een ontvangstbewijs tegen het paknummer.

21.3.2. *Overdracht binnen een gebouw of een groep gebouwen*

Binnen een gebouw of een groep gebouwen mogen gerubriceerde documenten worden vervoerd in een verzegelde enveloppe waarop alleen de naam van de geadresseerde voorkomt, mits de enveloppe wordt vervoerd door een persoon die voor de rubriceringsgraad van de documenten gemachtigd is.

21.3.3. *Overdracht binnen een land*

1. Binnen een land mogen ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten alleen worden vervoerd door een officiële koeriersdienst of door personen die gemachtigd zijn voor toegang tot ►M1 TRES SECRET UE/EU TOP SECRET ◄-gegevens.

2. Wanneer voor de overdracht van een ►M1 TRES SECRET UE/EU TOP SECRET ◄-document buiten een gebouw of een groep gebouwen gebruik wordt gemaakt van een koeriersdienst, moeten de bepalingen van dit hoofdstuk inzake verpakking en ontvangst worden nageleefd. Koeriersdiensten moeten zodanig zijn bemand dat pakketten met ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten te allen tijde onder de directe supervisie van een bevoegd persoon blijven.

3. In uitzonderlijke gevallen mogen andere ambtenaren dan bodes ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten uit een gebouw of groep gebouwen meenemen voor gebruik tijdens vergaderingen of besprekingen, op voorwaarde dat:

   a) de betrokken ambtenaar gemachtigd is voor toegang tot deze ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten;

   b) de wijze van transport voldoet aan de voorschriften voor de overdracht van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten;

   c) de betrokken ambtenaar de ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten in geen geval onbeheerd laat;

   d) erop wordt toegezien dat aldus vervoerde documenten die in het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register voorkomen, in een logboek worden genoteerd, en dat de terugkeer van de documenten aan de hand van deze gegevens wordt gecontroleerd.

4. Binnen een land mogen ►M1 SECRET UE ◄- en ►M1 CONFIDENTIEL UE ◄-documenten hetzij per post worden verzonden, indien de nationale regelgeving dat toestaat en die regelgeving wordt nageleefd, hetzij worden bezorgd via een koeriersdienst of door personen die gemachtigd zijn voor toegang tot de gerubriceerde EU-gegevens.

▼B

5. ►M2 Het directoraat Veiligheid van de Commissie ◄ stelt op basis van deze voorschriften instructies vast voor de personen die gerubriceerde EU-gegevens vervoeren. Deze instructies moeten door de drager van de documenten worden gelezen en ondertekend. In die instructies moet met name duidelijk zijn aangegeven dat de documenten in geen geval:

a) door de drager uit handen mogen worden gegeven, tenzij ze veilig worden opgeborgen overeenkomstig het bepaalde in afdeling 18;

b) onbeheerd mogen worden achtergelaten in openbare of particuliere voertuigen of op plaatsen als restaurants of hotels. Zij mogen niet in hotelkluizen worden bewaard of onbeheerd op hotelkamers worden achtergelaten;

c) mogen gelezen worden op openbare plaatsen als vliegtuigen of treinen.

21.3.4. *Overdracht van de ene staat naar de andere*

1. Materiaal met rubriceringsgraad ►M1 CONFIDENTIEL UE ◄ of hoger moet door diplomatieke of militaire koeriersdiensten worden vervoerd.

2. Vervoer door personen van als ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ gerubriceerd materiaal kan evenwel worden toegestaan, als de nodige voorzorgsmaatregelen worden genomen om te voorkomen dat het materiaal in handen van onbevoegden terechtkomt.

3. Het Commissielid dat bevoegd is voor veiligheidsaangelegenheden kan vervoer door personen toestaan wanneer geen diplomatieke of militaire koeriers beschikbaar zijn, of wanneer het gebruik van dergelijke koeriers tot een vertraging zou leiden die de EU-operaties kan schaden, en de geadresseerde het materiaal dringend nodig heeft. ►M2 Het directoraat Veiligheid van de Commissie ◄ stelt instructies op voor het internationaal vervoer van materiaal tot en met de rubriceringsgraad ►M1 SECRET UE ◄ door andere personen dan diplomatieke of militaire koeriers. Die instructies moeten het volgende voorschrijven:

a) de drager moet in het bezit zijn van een passende veiligheidsmachtiging;

b) de betrokken dienst of het betrokken register houdt een bestand bij van al het materiaal dat op die wijze vervoerd wordt;

c) op pakketten of zakken die EU-materiaal bevatten moet een officieel stempel ter voorkoming van douanecontroles zijn aangebracht alsmede etiketten met identificatiegegevens en instructies voor de eventuele vinder;

d) de drager moet in het bezit zijn van een door alle EU-lidstaten erkende koerierspas en/of dienstopdracht op grond waarvan hij gemachtigd is het daarin gespecificeerde pakket te vervoeren;

e) in geval van vervoer over land mag niet over het grondgebied worden gereisd van een staat die niet tot de EU behoort of mag de grens van een dergelijke staat niet worden overschreden, tenzij de lidstaat van verzending speciale garanties van deze staat heeft gekregen;

f) het reisplan, de reisroute en de keuze van de vervoermiddelen moeten voldoen aan de EU-voorschriften of aan de nationale voorschriften, indien deze strenger zijn;

g) de drager mag het materiaal niet uit handen geven, tenzij het veilig wordt opgeslagen overeenkomstig het bepaalde in afdeling 18;

h) het materiaal mag niet onbeheerd worden achtergelaten in openbare of particuliere voertuigen, of op plaatsen als restaurants en hotels. Het mag niet in hotelkluizen worden bewaard of onbeheerd in hotelkamers worden achtergelaten;

i) documenten die worden vervoerd mogen niet worden gelezen op openbare plaatsen (bv. vliegtuigen, treinen, enz.).

▼B

4. De persoon die met het vervoer van het gerubriceerd materiaal is belast, moet een document lezen en ondertekenen dat ten minste de bovenbedoelde instructies bevat en waarin de procedures zijn uiteengezet die moeten worden gevolgd in geval van nood of wanneer een pakket met gerubriceerd materiaal door de douane of door de veiligheidsdienst van een luchthaven wordt opgeëist.

21.3.5. *Overdracht van* ►M1 *RESTREINT UE* ◄ *documenten*

Voor het vervoer van documenten met rubriceringsgraad ►M1 RESTREINT UE ◄ gelden geen speciale voorschriften, behalve dat erop moet worden toegezien dat de documenten niet in handen van onbevoegden terechtkomen.

21.4. **Veiligheidsonderzoek van koeriers**

Koeriers en bodes die worden belast met het vervoer van documenten met rubriceringsgraad ►M1 SECRET UE ◄ en ►M1 CONFIDENTIEL UE ◄, moeten vooraf een passend veiligheidsonderzoek ondergaan.

21.5. **Elektronische en andere middelen van technische overdracht**

1. Er moeten communicatiebeveiligingsmaatregelen worden vastgesteld waarmee de veilige overdracht van gerubriceerde EU-gegevens kan worden gegarandeerd. Gedetailleerde voorschriften in dit verband zijn vermeld in afdeling 25.

2. Gegevens met rubriceringsgraad ►M1 CONFIDENTIEL UE ◄ of ►M1 SECRET UE ◄ mogen alleen door geaccrediteerde communicatiecentra en netwerken en/of terminals en systemen worden doorgezonden.

21.6. **Extra kopieën, vertalingen en uittreksels van gerubriceerde EU-documenten**

1. Alleen de opsteller mag toestemming geven voor het kopiëren of vertalen van documenten met rubriceringsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Wanneer gegevens die, hoewel ze in een ►M1 TRES SECRET UE/EU TOP SECRET ◄-document voorkomen, zelf een andere rubricering hebben, worden opgevraagd door personen die niet over een machtiging voor toegang tot ►M1 TRES SECRET UE/EU TOP SECRET ◄-informatie beschikken, kan het hoofd van het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register (zie 22.2) toestemming krijgen om het gevraagde aantal uittreksels uit dat document af te leveren. Daarbij moet hij/zij ervoor zorgen dat die uittreksels de passende rubriceringsgraad krijgen.

3. Documenten met rubriceringsgraad ►M1 SECRET UE ◄ of lager gerubriceerde mogen door de geadresseerde worden gereproduceerd of vertaald, binnen het kader van deze veiligheidsvoorschriften en op voorwaarde dat het „need-to-know”-beginsel strikt in acht wordt genomen. De veiligheidsmaatregelen die voor het originele document gelden, zijn ook van toepassing op de reproducties en/of vertalingen daarvan.

22. EUCI-REGISTERS, CONTROLES, ARCHIVERING EN VERNIETIGING VAN GERUBRICEERDE EU–GEGEVENS

22.1. **Plaatselijke registers van gerubriceerde EU-gegevens (EUCI-registers)**

1. Bij iedere dienst van de Commissie is, naar gelang van de behoeften, één of meer plaatselijke EUCI-registers bevoegd voor de registratie, de reproductie, de verzending, de archivering en de vernietiging van documenten met rubriceringsgraad ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄.

2. Voor diensten die niet over een plaatselijke EUCI-register beschikken, treedt het plaatselijk EUCI-register van het secretariaat-generaal op als zodanig.

3. De plaatselijke EUCI-registers brengen verslag uit bij het hoofd van de dienst van wie zij instructies krijgen. Aan het hoofd van deze registers staat de functionaris voor de registercontrole (RCO).

▼B

4. Zij staan onder toezicht van de plaatselijke veiligheidsfunctionaris wat betreft de toepassing van de voorschriften inzake de behandeling van EUCI-documenten en de uitvoering van de desbetreffende veiligheidsmaatregelen.

5. De ambtenaren van de plaatselijke EUCI-registers zijn gemachtigd om toegang te hebben tot de gerubriceerde EU-gegevens, overeenkomstig het bepaalde in afdeling 20.

6. De plaatselijke EUCI-registers zijn, onder toezicht van het hoofd van de dienst, belast met:

   a) het beheren van activiteiten in verband met het registreren, reproduceren, vertalen, overdragen, verzenden en vernietigen van de gegevens;

   b) het bijhouden van de lijst met bijzonderheden over de gerubriceerde gegevens;

   c) het op gezette tijden vaststellen of bepaalde gegevens gerubriceerd moeten blijven;

7. De plaatselijke EUCI-registers houden een register bij waarin de volgende bijzonderheden zijn vermeld:

   a) de datum van opstelling van de gerubriceerde gegevens;

   b) de rubriceringsgraad;

   c) de datum waarop de rubricering verstrijkt;

   d) de naam en de afdeling van de afzender;

   e) de geadresseerde(n), met volgnummer;

   f) het onderwerp;

   g) het aantal;

   h) het aantal verspreide kopieën;

   i) een inventaris van de gerubriceerde gegevens die aan de afdeling zijn meegedeeld;

   j) een register van de gederubriceerde en de lager gerubriceerde gegevens.

8. De algemene voorschriften als bedoeld in afdeling 21 zijn van toepassing op de plaatselijke EUCI-registers, voor zover ze door de bepalingen van deze afdeling niet zijn gewijzigd.

22.2. **Het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register**

22.2.1. *Algemeen*

1. Een centraal ►M1 TRES SECRET UE/EU TOP SECRET ◄ register zorgt voor het registreren, verwerken en verspreiden van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten overeenkomstig de veiligheidsvoorschriften. Aan het hoofd van ►M1 TRES SECRET UE/EU TOP SECRET ◄-register staat de controlefunctionaris voor de registratiecontrole (RCO).

2. Het centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄ register is bij de Commissie de belangrijkste autoriteit voor ontvangst en verzending ten aanzien van andere EU-instellingen, internationale organisaties en derde landen waarmee de Commissie overeenkomsten heeft gesloten inzake beveiligingsprocedures voor de uitwisseling van gerubriceerde gegevens.

3. Indien nodig worden subregisters opgezet voor het intern beheer van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten; deze subregisters houden bijgewerkte bestanden bij met betrekking tot de circulatie van de documenten waarvoor zij bevoegd zijn.

▼B

4. ►M1 TRES SECRET UE/EU TOP SECRET ◄ sub-registers worden opgezet overeenkomstig het bepaalde in afdeling 22.2.3; zij zijn op de lange termijn gericht en worden gekoppeld aan een centraal ►M1 TRES SECRET UE/EU TOP SECRET ◄-register. Wanneer er behoefte bestaat om ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten slechts tijdelijk en incidenteel te raadplegen, kunnen deze worden vrijgegeven zonder dat een ►M1 TRES SECRET UE/EU TOP SECRET ◄-subregister wordt opgezet, op voorwaarde dat maatregelen worden genomen om ervoor te zorgen dat deze documenten onder de controle van het betrokken ►M1 TRES SECRET UE/EU TOP SECRET ◄-register blijven en dat alle voorschriften inzake fysieke en personele beveiliging nageleefd worden.

5. Subregisters mogen geen ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten rechtstreeks overdragen aan andere subregisters van hetzelfde centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄-register zonder uitdrukkelijke toestemming van het centrale register.

6. Uitwisselingen van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten tussen subregisters die niet tot hetzelfde centrale register behoren, verlopen via de centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄-registers.

22.2.2. *Het centraal* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄*-register*

Als functionaris voor de registercontrole is het hoofd van het centraal ►M1 TRES SECRET UE/EU TOP SECRET ◄-register verantwoordelijk voor:

a) de overdracht van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten overeenkomstig het bepaalde in afdeling 21.3;

b) het bijhouden van een lijst van alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-subregisters die tot het centraal register behoren, en van de naam en de handtekening van de functionarissen voor de registercontrole en hun gemachtigde plaatsvervangers;

c) het bewaren van de ontvangstbewijzen van andere registers voor alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten die door het centrale register zijn verspreid;

d) het bijhouden van een overzicht van de ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten die bewaard worden en in omloop zijn;

e) het bijhouden van een bijgewerkte lijst van alle centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄-registers waarmee hij normaliter correspondeert, en van de naam en de handtekening van de functionarissen voor de registercontrole en hun gemachtigde plaatsvervangers;

f) de fysieke bewaking van alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten die in het register zijn opgenomen, overeenkomstig het bepaalde in afdeling 18.

22.2.3. ►M1 *TRES SECRET UE/EU TOP SECRET* ◄*-subregisters*

Als functionaris voor de registercontrole is het hoofd van een ►M1 TRES SECRET UE/EU TOP SECRET ◄-subregister verantwoordelijk voor:

a) de overdracht van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten overeenkomstig het bepaalde in afdeling 21.3;

b) het bijhouden van een lijst van alle personen die gemachtigd zijn om toegang te hebben tot de ►M1 TRES SECRET UE/EU TOP SECRET ◄-gegevens waarvoor hij verantwoordelijk is;

c) de verspreiding van ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten volgens de instructies van de instantie die de documenten verstrekt heeft of op een „need-to-know”-basis, nadat eerst is nagegaan of de geadresseerde de vereiste veiligheidsmachtiging heeft;

d) het bijhouden van een bijgewerkt overzicht van alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten die hij bewaart of die onder zijn toezicht in omloop zijn, of die aan andere ►M1 TRES SECRET UE/EU TOP SECRET ◄-registers zijn doorgegeven; het bewaren van alle corresponderende ontvangstbewijzen;

▼B

e) het bijhouden van een lijst van ►M1 TRES SECRET UE/EU TOP SECRET ◄-registers waarmee hij ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten mag uitwisselen en van de naam en de handtekening van de functionarissen voor de registercontrole en hun gemachtigde plaatsvervangers;

f) de fysieke bewaking van alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten die in het register zijn opgenomen, overeenkomstig het bepaalde in afdeling 18.

22.3. **Inventarisatie en controle van gerubriceerde EU-documenten**

1. Ieder jaar stelt elk ►M1 TRES SECRET UE/EU TOP SECRET ◄-register als bedoeld in deze afdeling, een gespecificeerde inventaris op van alle ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten. Een document wordt geacht tot een register te behoren wanneer dat document fysiek op het register aanwezig is, of wanneer het register in het bezit is van een ontvangstbewijs van het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register waaraan het document is overgedragen, van een proces-verbaal van vernietiging voor het document of van een opdracht om dat document lager te rubriceren of te derubriceren. De resultaten van de jaarlijkse inventaris worden ieder jaar uiterlijk op 1 april naar het Commissielid gezonden dat bevoegd is voor veiligheidsaangelegenheden.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄-subregisters zenden de resultaten van hun jaarlijkse inventaris toe aan het centraal register waaronder zij ressorteren, op een tijdstip dat door het centraal register wordt bepaald.

3. Documenten met een rubriceringsgraad lager dan ►M1 TRES SECRET UE/EU TOP SECRET ◄ worden aan interne controles onderworpen volgens de instructies van het Commissielid dat bevoegd is voor veiligheidsaangelegenheden.

4. Deze controles moeten het mogelijk maken na te gaan of:

   a) bepaalde documenten lager kunnen worden gerubriceerd of kunnen worden gederubriceerd;

   b) documenten moeten worden vernietigd.

22.4. **Archivering van gerubriceerde EU-gegevens**

1. Gerubriceerde EU-gegevens moeten worden opgeslagen overeenkomstig het bepaalde in afdeling 18.

2. Om opslagproblemen te voorkomen, kunnen de functionarissen voor de registercontrole documenten met rubriceringsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ voor archiveringsdoeleinden op microfilm vastleggen of met behulp van andere magnetische of optische middelen opslaan, op voorwaarde dat:

   a) de werkzaamheden worden verricht door personeelsleden die een geldige machtiging voor de desbetreffende rubriceringsgraad bezitten;

   b) de microfilm/gegevensdrager op dezelfde wijze beveiligd is als de originele documenten;

   c) de opsteller van het document van de verfilming of de opslag in kennis wordt gesteld;

   d) op ieder filmrolletje of op iedere andere gegevensdrager alleen documenten worden opgeslagen met dezelfde rubriceringsgraad (►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄);

▼B

e) in het bestand dat voor de jaarlijkse inventaris wordt gebruikt duidelijk is aangegeven welke ►M1 TRES SECRET UE/EU TOP SECRET ◄- of ►M1 SECRET UE ◄-documenten op microfilm zijn vastgelegd of op een andere gegevensdrager zijn opgeslagen;

f) de originelen van de verfilmde of opgeslagen documenten overeenkomstig het bepaalde in afdeling 22.5 worden vernietigd.

3. Deze voorschriften zijn ook van toepassing op andere toegelaten vormen van opslag, zoals elektromagnetische middelen en optische schijven.

22.5. **Vernietiging van gerubriceerde EU-gegevens**

1. Om onnodige accumulatie van gerubriceerde EU-documenten te voorkomen, moeten de documenten die door het hoofd van de dienst die ze bewaart, als achterhaald en overtollig worden beschouwd, zo spoedig mogelijk op onderstaande wijze worden vernietigd:

a) ►M1 TRES SECRET UE/EU TOP SECRET ◄ mogen alleen door het bevoegde centrale register worden vernietigd. Elk vernietigd document wordt genoteerd in een proces-verbaal van vernietiging, dat ondertekend wordt door de functionaris voor de registercontrole van het ►M1 TRES SECRET UE/EU TOP SECRET ◄-register en door de functionaris die bij de vernietiging aanwezig was en die over een machtiging voor rubriceringsgraad ►M1 TRES SECRET UE/EU TOP SECRET ◄ beschikt. Hiervan wordt aantekening gemaakt in het logboek.

b) Het register moet de processen-verbaal van vernietiging samen met de verspreidingsformulieren gedurende tien jaar bewaren. Alleen op uitdrukkelijk verzoek worden aan de opsteller van de documenten of aan het betrokken centrale register kopieën verstrekt.

c) ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten, alsmede alle daarmee verband houdende gerubriceerde nevenproducten, zoals kladversies, ontwerpteksten, getypte aantekeningen en diskettes, worden onder toezicht van een functionaris voor de registercontrole van een ►M1 TRES SECRET UE/EU TOP SECRET ◄-register vernietigd door verbranding, verpulping, versnippering of op een andere wijze waarbij de documenten onherkenbaar en onherstelbaar worden.

2. ►M1 SECRET UE ◄-documenten worden door het bevoegde register op een van de onder punt 1c bedoelde wijzen vernietigd, onder toezicht van een persoon met een veiligheidsmachtiging. Van de vernietigde ►M1 SECRET UE ◄-documenten wordt een proces-verbaal van vernietiging opgemaakt en ondertekend, dat samen met de verspreidingsformulieren gedurende ten minste drie jaar in het register wordt bewaard.

3. 33. ►M1 CONFIDENTIEL UE ◄-documenten worden door het bevoegde register op een van de onder punt 1c bedoelde wijzen vernietigd, onder toezicht van een persoon met een veiligheidsmachtiging. De vernietiging van deze documenten wordt geregistreerd volgens de instructies van het Commissielid dat bevoegd is voor veiligheidsaangelegenheden.

4. ►M1 RESTREINT UE ◄-documenten worden door het bevoegde register of door de gebruiker vernietigd, volgens de instructies van het Commissielid dat bevoegd is voor veiligheidsaangelegenheden.

22.6. **Vernietiging in noodgevallen**

1. De diensten van de Commissie stellen, naar gelang van de plaatselijke omstandigheden, plannen op ter beveiliging van gerubriceerd EU-materiaal in crisissituaties, die indien nodig noodvernietigings- en evacuatieplannen omvatten. In die plannen worden de instructies vastgesteld die nodig worden geacht om te voorkomen dat gerubriceerde EU-gegevens in handen van onbevoegden terechtkomen.

▼B

2. De regelingen die in crisissituaties worden getroffen om materiaal met rubriceringsgraad ►M1 SECRET UE ◄ of ►M1 CONFIDENTIEL UE ◄ te beveiligen en/of te vernietigen, mogen in geen geval ten koste gaan van de beveiliging of de vernietiging van ►M1 TRES SECRET UE/EU TOP SECRET ◄-materiaal, inclusief de encryptieapparatuur, waarvan de werking voorrang heeft op alle andere taken.

3. De maatregelen voor de beveiliging en vernietiging van encryptieapparatuur in noodsituaties worden op grond van ad hoc instructies vastgesteld.

4. De instructies moeten onmiddellijk beschikbaar in een verzegelde enveloppe ter beschikking worden gesteld. De middelen en de technische uitrusting voor de vernietiging moeten beschikbaar zijn.

23. VEILIGHEIDSMAATREGELEN VOOR SPECIFIEKE VERGADERINGEN DIE BUITEN DE COMMISSIE WORDEN GEHOUDEN EN WAARBIJ GERUBRICEERDE EU–GEGEVENS ZIJN BETROKKEN

23.1. **Algemeen**

Wanneer vergaderingen van de Commissie of andere belangrijke bijeenkomsten buiten de gebouwen van de Commissie plaatsvinden, waarbij de hoge gevoeligheid van de behandelde aangelegenheden of gegevens bijzondere veiligheidseisen vereisen, dienen de hieronder beschreven veiligheidsmaatregelen te worden getroffen. Deze maatregelen hebben alleen betrekking op de bescherming van gerubriceerde EU-gegevens; er moeten wellicht ook andere veiligheidsmaatregelen worden overwogen.

23.2. **Verantwoordelijkheid**

23.2.1. ►M2 *Het directoraat Veiligheid van de Commissie* ◄

►M2 Het directoraat Veiligheid van de Commissie ◄ werkt met de bevoegde instanties van de lidstaat op wiens grondgebied de vergadering plaatsvindt (de gastlidstaat) samen om tijdens vergaderingen van de Commissie of andere belangrijke bijeenkomsten de veiligheid van de delegaties en van het personeel te garanderen. Het Veiligheidsbureau dient er in het bijzonder voor te zorgen dat:

a) plannen worden opgesteld om veiligheidsrisico's en veiligheidsincidenten aan te pakken, waarbij er in het bijzonder wordt op toegezien dat gerubriceerde EU-documenten veilig worden opgeborgen;

b) maatregelen worden getroffen om de toegang tot de communicatiesystemen van de Commissie mogelijk te maken, zodat gerubriceerde EU-berichten kunnen worden ontvangen en verstuurd. De gastlidstaat stelt desgewenst beveiligde telefoonsystemen ter beschikking.

Het Veiligheidsbureau geeft beveiligingsadviezen bij de voorbereiding van de vergadering; het is in de vergadering vertegenwoordigd en staat de beveiligingsfunctionaris van de vergadering en de delegaties waar nodig met raad en daad bij.

Elke delegatie in de vergadering dient een beveiligingsfunctionaris aan te wijzen, die binnen zijn delegatie verantwoordelijk is voor veiligheidskwesties en in contact staat met de beveiligingsfunctionaris van de vergadering en met de vertegenwoordiger van ►M2 het directoraat Veiligheid van de Commissie ◄, indien zulks nodig is.

23.2.2. *Beveiligingsfunctionaris van de vergadering (Meeting Security Officer - MSO)*

Er wordt een beveiligingsfunctionaris aangewezen, die verantwoordelijk is voor de algemene voorbereiding van en het toezicht op de algemene interne veiligheidsmaatregelen, alsook voor de coördinatie met de andere betrokken veiligheidsinstanties. De maatregelen die de beveiligingsfunctionaris treft hebben in het algemeen betrekking op:

a) beschermingsmaatregelen op de vergaderplaats, om ervoor te zorgen dat zich tijdens de vergadering geen incidenten voordoen die de beveiliging van gerubriceerde EU-gegevens die in de vergadering worden gebruikt, in gevaar kunnen brengen;

▼B

b) controle van het personeel dat toegang heeft tot de vergaderplaats, de delegatieruimten en de conferentieruimten, en controle van de apparatuur;

c) permanente coördinatie met de bevoegde autoriteiten van de gastlidstaat en met ►M2 het directoraat Veiligheid van de Commissie ◄;

d) het opnemen in het vergaderdossier van de veiligheidsinstructies, met inachtneming van deze voorschriften en van andere veiligheidsinstructies die nodig worden geacht.

23.3. **Veiligheidsmaatregelen**

23.3.1. *Veiligheidszones*

De volgende veiligheidszones dienen te worden ingesteld:

a) een veiligheidszone van klasse II, bestaande uit een redactieruimte, de ruimten van de Commissie en reproductieapparatuur, alsmede de delegatieruimten in voorkomend geval;

b) een veiligheidszone van klasse I, bestaande uit de conferentieruimte alsmede de tolkencabines en de werkruimte van de geluidstechnici;

c) administratieve zones, bestaande uit de persruimte en de delen van de vergaderlocatie die worden gebruikt ten behoeve van administratie, catering en accommodatie, alsmede de zone die grenst aan het perscentrum en de vergaderlocatie.

23.3.2. *Pasjes*

De veiligheidsfunctionaris voor de vergadering (MSO) dient de delegaties op hun verzoek van de nodige pasjes te voorzien. Indien nodig kan een onderscheid worden gemaakt naar gelang van de toegang tot verschillende veiligheidszones.

De veiligheidsinstructies voor de vergadering dienen te vereisen dat alle betrokkenen te allen tijde duidelijk zichtbaar hun pasje dragen op de vergaderlocatie, zodat zij zo nodig door het veiligheidspersoneel kunnen worden gecontroleerd.

Afgezien van de deelnemers die een pasje hebben, worden zo weinig mogelijk personen tot de vergaderlocatie toegelaten. De MSO mag alleen nationale delegaties die erom verzoeken, toestaan bezoekers te ontvangen tijdens de vergadering. Bezoekers dienen te worden voorzien van een bezoekerspasje. Voor het bezoekerspasje dient een registratiebewijs te worden ingevuld met daarop de naam van de bezoeker en van de persoon die wordt bezocht. Bezoekers dienen te allen tijde te worden begeleid door veiligheidspersoneel of door de bezochte persoon. De begeleidende persoon dient het registratiebewijs bij zich te houden en het, samen met het bezoekerspasje, terug te geven aan het veiligheidspersoneel wanneer de bezoeker de vergaderlocatie verlaat.

23.3.3. *Controle van foto- en audioapparatuur*

In een veiligheidszone van klasse I mogen geen camera's of opnameapparatuur worden binnengebracht, met uitzondering van apparatuur van fotografen en geluidstechnici die daartoe door de MSO gemachtigd zijn.

23.3.4. *Controle van aktetassen, draagbare computers en pakjes*

Aktetassen en draagbare computers (alleen indien voorzien van een autonome energiebron) van houders van pasjes die toegang hebben tot een veiligheidszone, worden normaliter niet gecontroleerd bij het betreden van die zone. Delegaties mogen voor hen bestemde pakjes in ontvangst nemen; die pakjes worden gecontroleerd door de veiligheidsfunctionaris van de betreffende delegatie, gescreend met speciale apparatuur of voor controle geopend door het veiligheidspersoneel. Indien de MSO voor de vergadering zulks nodig acht, kunnen strengere maatregelen met betrekking tot de controle van aktetassen en pakjes worden vastgelegd.

▼B

23.3.5. *Technische beveiliging*

De vergaderruimte kan „technisch veilig” worden gemaakt door een team voor technische beveiliging, dat tijdens de vergadering eveneens voor elektronisch toezicht kan zorgen.

23.3.6. *Documenten van delegaties*

De delegaties zijn verantwoordelijk voor het meenemen van gerubriceerde EU-documenten naar en van vergaderingen. Zij zijn tevens verantwoordelijk voor de controle en de beveiliging van zulke documenten wanneer zij die in de hun toegewezen ruimten gebruiken. De gastlidstaat kan om hulp worden verzocht voor het vervoer van gerubriceerde documenten van en naar de vergaderlocatie.

23.3.7. *Veilig opbergen van documenten*

Indien de Commissie of de delegaties hun gerubriceerde documenten niet conform goedgekeurde normen kunnen bewaren, mogen zij deze documenten, tegen ontvangstbewijs, in een verzegelde enveloppe aan de veiligheidsfunctionaris voor de vergadering overhandigen zodat deze functionaris de documenten conform goedgekeurde normen kan opbergen.

23.3.8. *Controle van ruimten*

De veiligheidsfunctionaris voor de vergadering dient erop toe te zien dat de ruimten van de Commissie en van de delegaties aan het einde van elke werkdag worden gecontroleerd, teneinde te garanderen dat gerubriceerde EU-documenten op een veilige plaats worden bewaard. Indien dat niet het geval is, dient hij/zij de nodige maatregelen te treffen.

23.3.9. *Verwijdering van afval van gerubriceerd EU-materiaal*

Afval dient te worden behandeld als gerubriceerd EU-materiaal, en papiermanden of -zakken moeten aan de Commissie en de delegaties ter beschikking worden gesteld om afval te verwijderen. Alvorens de hun toegewezen ruimten te verlaten, dienen de Commissie en de delegaties hun afval aan de veiligheidsfunctionaris voor de vergadering te overhandigen, die ervoor zorgt dat het afval volgens de regels wordt vernietigd.

Na afloop van de vergadering dienen alle documenten van de Commissie of van de delegaties die zij niet langer wensen te behouden, als afval te worden behandeld. De ruimten die de Commissie en de delegaties ter beschikking waren gesteld, moeten grondig worden gecontroleerd alvorens de voor de vergadering getroffen veiligheidsmaatregelen worden opgeheven. Documenten waarvoor een ontvangstbewijs was getekend, dienen, voorzover van toepassing, te worden vernietigd zoals beschreven in 22.5.

24. INBREUKEN OP DE VEILIGHEIDSVOORSCHRIFTEN EN COMPROMITTERING VAN GERUBRICEERDE EU-GEGEVENS

24.1. **Definities**

Een inbreuk op de veiligheidsvoorschriften is het resultaat van een handeling of een nalatigheid, in strijd met veiligheidsvoorschriften van de Commissie, die gerubriceerde EU-gegevens in gevaar kan brengen of compromitteren.

Compromittering van gerubriceerde EU-gegevens doet zich voor wanneer het zeker of aannemelijk is dat zulke gegevens geheel of gedeeltelijk in het bezit zijn gekomen van onbevoegden, d.w.z. personen die niet over de vereiste machtiging of „need-to-know” beschikken.

Gerubriceerde EU-gegevens kunnen gecompromitteerd zijn als gevolg van slordigheid, onachtzaamheid of indiscretie, alsmede, wat gerubriceerde EU-gegevens en -activiteiten betreft, door activiteiten van diensten die gericht zijn tegen de EU of haar lidstaten, dan wel door activiteiten van subversieve organisaties.

24.2. **Melding van inbreuken op veiligheidsvoorschriften**

Alle personen die gerubriceerde EU-gegevens moeten verwerken, moeten grondig worden geïnformeerd over hun verantwoordelijkheden op dit vlak. Zij moeten elke inbreuk op de veiligheidsvoorschriften waarvan zij kennis krijgen, onverwijld melden.

▼B

Indien een plaatselijke veiligheidsfunctionaris of een veiligheidsfunctionaris voor de vergadering een inbreuk op de veiligheidsvoorschriften met betrekking tot gerubriceerde EU-gegevens, dan wel het verlies of verdwijnen van gerubriceerd EU-materiaal ontdekt of daarvan in kennis wordt gesteld, doet hij/zij tijdig het nodige om:

a) bewijsmateriaal veilig te stellen;

b) de feiten vast te stellen;

c) de aangerichte schade te beoordelen en te beperken;

d) herhaling van de feiten te voorkomen;

e) de bevoegde autoriteiten in kennis te stellen van de gevolgen van de inbreuk op de veiligheidsvoorschriften.

In dat verband wordt de volgende informatie verstrekt:

i) een beschrijving van de betreffende gegevens, met inbegrip van de rubricering ervan, het referentie- en het kopienummer, de datum, de opsteller, het onderwerp en de verspreiding;

ii) een beknopte beschrijving van de omstandigheden van de inbreuk, met inbegrip van de datum en de periode gedurende welke de informatie aan compromittering was blootgesteld;

iii) een verklaring dat de opsteller al dan niet op de hoogte is gebracht.

De veiligheidsautoriteiten hebben tot taak om, zodra zij kennis krijgen van een mogelijke inbreuk op de veiligheidsvoorschriften, dit onmiddellijk te melden aan ►**M2** het directoraat Veiligheid van de Commissie ◄.

Gevallen waarbij als ►**M1** RESTREINT UE ◄ gerubriceerde gegevens betrokken zijn, behoeven alleen te worden gemeld indien zij ongewone aspecten vertonen.

Wanneer de voor veiligheid verantwoordelijke Commissaris in kennis wordt gesteld van een inbreuk op de veiligheidsvoorschriften:

a) stelt hij de autoriteit waarvan de betreffende gerubriceerde gegevens afkomstig zijn, daarvan in kennis;

b) verzoekt hij de bevoegde veiligheidsautoriteiten een onderzoek in te stellen;

c) coördineert hij het onderzoek, indien er meer dan één veiligheidsautoriteit bij betrokken is;

d) wordt aan hem gerapporteerd over de omstandigheden van de inbreuk, de datum of de periode waarin de inbreuk zich kan hebben voorgedaan, en de ontdekking van de inbreuk, met een gedetailleerde beschrijving van de inhoud en de rubriceringsgraad van het betreffende materiaal. Voorts moet ook de schade aan belangen van de EU of van een of meer van haar lidstaten worden gerapporteerd, alsmede de stappen die zijn ondernomen om herhaling te voorkomen.

De opsteller van de gegevens dient de geadresseerden in te lichten en passende instructies te geven.

24.3. **Gerechtelijke actie**

Eenieder die verantwoordelijk is voor het compromitteren van gerubriceerde EU-gegevens stelt zich bloot aan disciplinaire maatregelen, overeenkomstig de geldende regels en voorschriften, met name overeenkomstig titel VI van het ambtenarenstatuut. Dit sluit verdere gerechtelijke actie niet uit.

In voorkomend geval moet de met veiligheid belaste Commissaris op basis van het in afdeling 24.2 bedoelde verslag de nodige stappen zetten om het de bevoegde nationale autoriteiten mogelijk te maken strafrechtelijke procedures in te leiden.

▼B

25. BESCHERMING VAN GERUBRICEERDE EU-GEGEVENS DIE VERWERKT WORDEN IN IT- EN COMMUNICATIEYSTEMEN

25.1. **Inleiding**

25.1.1. *Algemeen*

Het beleid en de vereisten inzake veiligheid zijn van toepassing op alle communicatie- en informatiesystemen en netwerken (hierna systemen genoemd) waarin als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens worden verwerkt. Zij gelden als aanvulling bij Besluit C (95) 1510 def. van de Commissie van 23 november 1995 inzake de beveiliging van informatiesystemen.

Systemen waarin als ►M1 RESTREINT UE ◄ gerubriceerde gegevens worden verwerkt, behoeven veiligheidsmaatregelen om het vertrouwelijke karakter van die gegevens te beschermen. Alle systemen behoeven veiligheidsmaatregelen ter bescherming van hun integriteit en beschikbaarheid en van de gegevens die zij bevatten.

Het door de Commissie toegepaste IT-beveiligingsbeleid omvat de volgende elementen:

— het is een integrerend onderdeel van de algemene veiligheidsregeling en completeert al de onderdelen van gegevensbeveiliging, personeelsgerelateerde en fysieke beveiliging,

— verdeling van de verantwoordelijkheden over eigenaars technische systemen, eigenaars van opgeslagen of in technische systemen verwerkte EUCI, beveiligingsspecialisten en gebruikers van IT,

— beschrijving van veiligheidsprincipes en vereisten voor elk IT-systeem,

— goedkeuring van deze principes en vereisten door een erkende autoriteit,

— waarbij rekening wordt gehouden met de specifieke bedreigingen en kwetsbaarheden van IT.

25.1.2. *Bedreigingen en kwetsbaarheden van systemen*

Een bedreiging kan in algemene zin worden gedefinieerd als een mogelijkheid om de beveiliging al dan niet opzettelijk te compromitteren. In het geval van systemen houdt zulks in dat een of meer van de volgende eigenschappen verloren gaan: vertrouwelijk karakter, integriteit of beschikbaarheid. Kwetsbaarheid kan worden gedefinieerd als onvoldoende of ontbrekende controles, waardoor bedreiging van een specifiek element of doel wordt vergemakkelijkt of mogelijk wordt.

Gerubriceerde en niet-gerubriceerde EU-gegevens die in een geconcentreerde vorm worden verwerkt in systemen zodat zij snel kunnen worden opgevraagd, overgedragen en gebruikt, staan aan velerlei bedreigingen bloot. Het kan onder meer gaan om toegang tot gegevens door niet-gemachtigde personen of juist om weigering van toegang aan gemachtigde gebruikers. Verder bestaat het risico van bekendmaking zonder machtiging, beschadiging, wijziging of vernietiging van gegevens. Bovendien is de complexe en soms fragiele apparatuur duur en dikwijls moeilijk snel te herstellen of te vervangen.

25.1.3. *Voornaamste doel van veiligheidsmaatregelen*

De in deze afdeling genoemde veiligheidsmaatregelen strekken er in de eerste plaats toe bescherming te bieden tegen openbaarmaking zonder machtiging (verlies van het vertrouwelijk karakter) en verlies van integriteit en beschikbaarheid van gerubriceerde EU-gegevens. Om een afdoende beveiliging van een systeem waarin gerubriceerde EU-gegevens worden verwerkt, te kunnen verwezenlijken, worden de toepasselijke conventionele veiligheidsnormen door ►M2 het directoraat Veiligheid van de Commissie ◄ gespecificeerd, samen met bijzondere beveiligingsprocedures en -technieken die op de respectieve systemen zijn afgestemd.

▼B

25.1.4. *Systeemgebonden specificatie van beveiligingseisen (SSRS)*

Voor alle systemen waarin als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens worden verwerkt, moet door de Eigenaar van het technisch systeem (TSO, zie 25.3.4) en de Informatie-eigenaar (zie 25.3.5), met de inbreng en bijstand van het projectteam en ►M2 het directoraat Veiligheid van de Commissie ◄ (Infosec-autoriteit — IA, zie 25.3.3), een Systeemgebonden Specificatie van Beveiligingseisen (SSRS) worden opgesteld en door de Autoriteit voor veiligheidsaccreditatie (SAA, zie 25.3.2) worden goedgekeurd.

Een SSRS is eveneens vereist indien de Autoriteit voor veiligheidsaccreditatie (SAA) de beschikbaarheid en integriteit van als ►M1 RESTREINT UE ◄ gerubriceerde of niet-gerubriceerde gegevens cruciaal acht.

De SSRS wordt zo vroeg mogelijk in de conceptfase van het project geformuleerd en wordt ontwikkeld en uitgebreid naarmate het project wordt ontwikkeld; de SSRS heeft diverse functies op diverse momenten in de looptijd van het project en de levensduur van het systeem.

25.1.5. *Beveiligingsmodi*

Alle systemen waarin als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens worden verwerkt, worden geaccrediteerd, zodat zij volgens een of — indien specifieke eisen op verschillende momenten zulks rechtvaardigen — meer van de volgende beveiligingsmodi of het nationale equivalent ervan functioneren:

a) „dedicated”,

b) „system high”, en

c) „multi level”.

25.2. **Definities**

Onder „accreditatie” wordt verstaan: de machtiging en goedkeuring die aan een systeem wordt verleend met het oog op de verwerking van gerubriceerde EU-gegevens in de operationele omgeving van dat systeem.

Opmerkingen:

Accreditatie vindt plaats nadat alle toepasselijke beveiligingsprocedures hun beslag hebben gekregen en het niveau van bescherming van de systeemmiddelen toereikend geacht wordt. Accreditatie dient normaliter te gebeuren op basis van de SSRS, alsmede van:

a) een verklaring inzake het doel van de accreditatie voor het systeem; in het bijzonder de rubriceringsgraad/-graden van de te verwerken gegevens en de voorgestelde wijze van beveiliging van het systeem of netwerk;

b) een evaluatie van de risicobeheersing, teneinde bedreigingen en kwetsbaarheden in kaart te brengen, alsmede maatregelen om die te verhelpen;

c) de Operationele Beveiligingsprocedures (SecOP's), met een gedetailleerde beschrijving van de voorgestelde operaties (bv. benodigde modi en diensten), alsmede een beschrijving van de beveiligingsvoorzieningen van het systeem waarop de accreditatie dient te worden gebaseerd;

d) het plan voor de installatie en het onderhoud van de beveiligingsvoorzieningen;

e) het plan voor initiële en opvolgtests in verband met de systeem- of netwerkbeveiliging, de evaluatie en certificatie, en

f) certificatie, zo nodig met andere accreditatie-elementen.

▼B

Onder „Centrale informatiebeveiligingsfunctionaris” (CISO) wordt verstaan: de functionaris in een centrale IT-dienst die beveiligingsmaatregelen voor centraal bestuurde diensten coördineert en daarop toezicht houdt.

Onder „certificatie” wordt verstaan: een formele verklaring, op grond van een onafhankelijke verificatie van een evaluatie en de resultaten ervan, over de mate waarin een systeem aan de beveiligingseisen voldoet, of over de doeltreffendheid van een product voor computerbeveiliging.

Onder „communicatiebeveiliging” (Comsec) wordt verstaan: de toepassing van veiligheidsmaatregelen op telecommunicatie, met de bedoeling niet-gemachtigden de toegang te ontzeggen tot gegevens waarvan de waarde kan voortvloeien uit het bezit en het bestuderen van dergelijke telecommunicatie, dan wel de authenticiteit van dergelijke telecommunicatie te verzekeren.

Opmerkingen:

Zulke maatregelen omvatten beveiliging op het gebied van versleuteling, doorzending en verspreiding, en betreffen ook procedurele, fysieke, personeelsgerelateerde, document- en computerbeveiliging.

Onder „computerbeveiliging” (Compusec) wordt verstaan: de toepassing van beveiligingsvoorzieningen op het gebied van hardware, firmware en software op een computersysteem, met de bedoeling bescherming te bieden tegen openbaarmaking zonder machtiging, manipulatie, wijziging/vernietiging van gegevens of niet-functioneren, dan wel zulks te voorkomen.

Onder „product voor computerbeveiliging” wordt verstaan: een generiek beveiligingselement voor computers dat in een IT-systeem wordt geïntegreerd met de bedoeling het vertrouwelijke karakter, de integriteit of de beschikbaarheid van de verwerkte gegevens te versterken of te verzekeren.

Onder de beveiligingsmodus „dedicated” wordt verstaan: een modus operandi waarbij ALLE personen die toegang hebben tot het systeem een machtiging hebben voor de hoogste graad van rubricering van de in het systeem verwerkte gegevens en tevens een gedeelde „need-to-know” voor ALLE in het systeem verwerkte gegevens.

Opmerkingen:

(1) Gedeelde „need-to-know”: impliceert dat de beveiligingsvoorzieningen van de computer niet hoeven te voorzien in scheiding van de gegevens in het systeem.

(2) Andere beveiligingsvoorzieningen (bv. fysieke, personeelsgerelateerde en procedurele voorzieningen) moeten overeenstemmen met de eisen van de hoogste rubriceringsgraad en alle categoriebenamingen van de in het systeem verwerkte gegevens.

Onder „evaluatie” wordt verstaan: een gedetailleerd technisch onderzoek door een bevoegde autoriteit van de veiligheidsaspecten van een systeem of van een product voor versleuteling of computerbeveiliging.

Opmerkingen:

(1) In het kader van een evaluatie wordt onderzocht of de beveiliging voldoende efficiënt is, wordt nagegaan of die doelmatigheid geen schadelijke neveneffecten heeft en wordt de integriteit ervan beoordeeld.

(2) In het kader van een evaluatie wordt bepaald in welke mate aan de beveiligingseisen van een systeem of aan de in het vooruitzicht gestelde beveiliging van een product voor computerbeveiliging wordt voldaan, en wordt het niveau van betrouwbaarheid van het systeem of van de „trusted function” van de versleuteling, dan wel van het product voor computerbeveiliging vastgesteld.

Onder „informatie-eigenaar” (IO) wordt verstaan: de autoriteit (afdelingshoofd) die verantwoordelijk is voor het creëren, verwerken en gebruiken van informatie, alsmede voor het aanwijzen van de personen die toegang tot die informatie kunnen krijgen.

▼B

Onder „informatiebeveiliging” (Infosec) wordt verstaan: het toepassen van veiligheidsmaatregelen met de bedoeling in communicatie-, informatie- en andere elektronische systemen verwerkte, opgeslagen of doorgezonden gegevens te beschermen tegen al dan niet opzettelijke aantasting van vertrouwelijk karakter, integriteit of beschikbaarheid, en aantasting van de integriteit en beschikbaarheid van de systemen zelf te voorkomen.

„Infosec-maatregelen” omvatten maatregelen op het gebied van beveiliging van computers, doorzending, terbeschikkingstelling en versleuteling, alsmede de opsporing en documentering van en de beveiliging tegen risico's voor gegevens en systemen.

Onder „IT-zone” wordt verstaan: een zone die een of meer computers bevat, de lokale perifere en opslagunits daarvan, de controle-units en de specifieke netwerk- en communicatieapparatuur.

Opmerkingen:

Dit slaat niet op een aparte zone waarin zich afzonderlijke perifere voorzieningen of terminals/werkstations bevinden, ook al zijn de bedoelde voorzieningen verbonden met apparatuur in de IT-zone.

Onder „IT-netwerk” wordt verstaan: de geografisch gespreide organisatie van onderling verbonden IT-systemen met het oog op de uitwisseling van gegevens, bestaande uit de bestanddelen van de gekoppelde IT-systemen en hun interface met de ondersteunende gegevens- of communicatienetwerken.

Opmerkingen:

(1) Een IT-netwerk kan gebruik maken van de diensten van een of meer gekoppelde communicatienetwerken om gegevens uit te wisselen; verschillende IT-netwerken kunnen gebruik maken van de diensten van een gemeenschappelijk communicatienetwerk.

(2) Een IT-netwerk wordt „lokaal” genoemd, indien het verschillende computers verbindt op dezelfde locatie.

De „Beveiligingsvoorzieningen van een IT-netwerk” omvatten de IT-systeembeveiligingsvoorzieningen van de respectieve IT-systemen die samen het netwerk vormen, samen met de additionele componenten en voorzieningen die met het netwerk als dusdanig zijn verbonden (bv. netwerkcommunicatie, veiligheidsidentificatie en markeringsmechanismen en -procedures, toegangscontroles, programma's en „audit trails”) en die nodig zijn om een aanvaardbaar niveau van bescherming voor gerubriceerde gegevens te bieden.

Onder „IT-systeem” wordt verstaan: de organisatie van een geheel van apparatuur, methodes en procedures, en, zo nodig, personeel, met het doel functies op het gebied van gegevensverwerking uit te voeren.

Opmerkingen:

(1) Hieronder moet worden verstaan, een geheel van faciliteiten in een configuratie die gericht is op de verwerking van gegevens in het systeem.

(2) Zulke systemen kunnen dienen ter ondersteuning van applicaties voor raadpleging, besturing, controle of communicatie, dan wel wetenschappelijke of administratieve applicaties, met inbegrip van tekstverwerking.

(3) De begrenzing van een systeem wordt doorgaans gedefinieerd als zijnde de elementen die door één enkele TSO worden gecontroleerd.

(4) Een IT-systeem kan subsystemen bevatten die op hun beurt IT-systemen zijn.

▼B

„Beveiligingsvoorzieningen van een IT-systeem" bestaan uit alle hardware/firmware/software-functies, -kenmerken en -voorzieningen; operationele procedures, procedures inzake verantwoordelijkheid en toegangscontrole, de IT-zone, de zone met afzonderlijke terminals/werkstations en de beheerseisen; fysieke structuur en voorzieningen, alsmede de controle van personeel en communicatie die nodig is om een aanvaardbaar niveau van bescherming van de in een IT-systeem te verwerken gegevens te bieden.

Onder „plaatselijke informatiebeveiligingsfunctionaris" (LISO) wordt verstaan: de functionaris in een dienst van de Commissie die verantwoordelijk is voor de coördinatie van en het toezicht op de beveiligingsmaatregelen in zijn domein.

Onder de beveiligingsmodus „Multi-level" wordt verstaan: een modus operandi waarbij NIET ALLE personen die toegang hebben tot het systeem, een machtiging hebben voor de hoogste graad van rubricering van de in het systeem verwerkte gegevens, en NIET ALLE personen met toegang tot het systeem een gedeelde „need-to-know" hebben voor de in het systeem verwerkte gegevens.

Opmerkingen:

(1) Met deze modus operandi kunnen momenteel gegevens met verschillende rubriceringsgraden en uiteenlopende categoriebenamingen worden verwerkt.

(2) Het feit dat niet alle personen een machtiging hebben tot de hoogste graad en er geen gedeelde „need-to-know" is, impliceert dat de beveiliging van de computer moet voorzien in een selectieve toegang tot en scheiding van gegevens in het systeem.

Onder „zone met afzonderlijke terminals/werkstations" wordt verstaan: een zone die computerapparatuur bevat, de lokale perifere voorzieningen of terminals/werkstations daarvan en alle daarmee verband houdende communicatieapparatuur, dit alles gescheiden van een IT-zone.

Onder „operationele beveiligingsprocedures" wordt verstaan: de procedures die door de TSO worden opgesteld en waarin de inzake beveiliging te hanteren principes zijn vastgesteld, alsmede de te volgen procedures en de verantwoordelijkheden van het personeel.

Onder de beveiligingsmodus „System-high" wordt verstaan: een modus operandi waarbij ALLE personen die toegang hebben tot het systeem, een machtiging hebben voor de hoogste graad van rubricering van de in het systeem verwerkte gegevens, maar NIET ALLE personen met toegang tot het systeem een gedeelde „need-to-know" hebben voor de in het systeem verwerkte gegevens.

Opmerkingen:

(1) Indien er geen gedeelde „need-to-know" is, impliceert dit dat de beveiligingsvoorzieningen van de computer moeten voorzien in selectieve toegang tot en scheiding van gegevens in het systeem.

(2) Andere beveiligingsvoorzieningen (bv. fysieke, personeelsgerelateerde en procedurele voorzieningen) moeten overeenstemmen met de eisen van de hoogste rubriceringsgraad en alle categoriebenamingen van de in het systeem verwerkte gegevens.

(3) Alle op grond van deze modus operandi in een systeem verwerkte of beschikbare gegevens, alsmede de gegenereerde output, worden, tot anders wordt bepaald, beschermd als gold het de categoriebenaming en de hoogste rubriceringsgraad van de verwerkte gegevens tenzij de bestaande markeringsfuncties voldoende betrouwbaar zijn.

▼B

Een „Systeemgebonden Specificatie van Beveiligingseisen" (SSRS) is een volledige en uitdrukkelijke verklaring over de beveiligingsprincipes die in acht moeten worden genomen en de gedetailleerde beveiligingseisen waaraan moet worden voldaan. De SSRS is gebaseerd op het beveiligingsbeleid en de risicobeoordeling van de Commissie, of vloeit voort uit parameters met betrekking tot de operationele omgeving, de laagste machtigingsgraad van het betrokken personeel, de hoogste rubriceringsgraad van de verwerkte gegevens, de beveiligingsmodi of gebruikerseisen. De SSRS vormt een integrerend onderdeel van de projectdocumentatie die aan de bevoegde autoriteiten moet worden voorgelegd met het oog op technische, budgettaire en veiligheidsgoedkeuring. In zijn definitieve vorm geeft de SSRS uitsluitsel over wat onder een veilig systeem moet worden verstaan.

Onder „Eigenaar technisch systeem" (TSO) wordt verstaan: de autoriteit die verantwoordelijk is voor het creëren, onderhouden, bedienen en afsluiten van een systeem.

Anti-Tempest-maatregelen: beveiligingsmaatregelen die erop gericht zijn apparatuur en communicatie-infrastructuur te beschermen tegen het compromitteren van gerubriceerde gegevens door onopzettelijke elektromagnetische emissies en door geleiding.

25.3. **Verantwoordelijkheden in verband met beveiliging**

25.3.1. *Algemeen*

De adviserende rol van de Adviesgroep Beveiligingsbeleid van de Commissie, als omschreven in afdeling 12 heeft ook betrekking op Infosec-thema's. De Adviesgroep organiseert zijn werkzaamheden zodanig dat het deskundig advies over bovengenoemde aangelegenheden kan verstrekken.

►**M2** Het directoraat Veiligheid van de Commissie ◄ heeft tot taak nadere bepalingen inzake Infosec vast te stellen overeenkomstig de bepalingen in dit hoofdstuk.

In geval van beveiligingsproblemen (incidenten, inbreuken, enz.) treedt ►**M2** het directoraat Veiligheid van de Commissie ◄ onmiddellijk op.

►**M2** Het directoraat Veiligheid van de Commissie ◄ moet voor Infosec een aparte eenheid omvatten.

25.3.2. *De Autoriteit voor veiligheidsaccreditatie (SAA)*

►**M2** De directeur van het directoraat Veiligheid van de Commissie ◄ is de autoriteit voor Veiligheidsaccreditatie (SAA) voor de Commissie. De SAA is verantwoordelijk voor beveiliging in het algemeen en voor Infosec, Communicatiebeveiliging, versleutelingsbeveiliging en „Tempest"-beveiliging in het bijzonder.

De SAA moet ervoor zorgen dat de systemen voldoen aan het beveiligingsbeleid van de Commissie. Een van de taken is een systeem de goedkeuring te verlenen om gerubriceerde EU-gegevens in zijn operationele omgeving te verwerken, naar gelang van het vastgestelde rubriceringsniveau.

De bevoegdheid van de SAA van de Commissie omvat alle in de gebouwen van de Commissie functionerende systemen. Indien verschillende bestanddelen van een systeem onder de bevoegdheid van de SAA van de Commissie en andere SAA's komen te vallen, wijzen alle partijen een gemeenschappelijk accreditatieorgaan aan, dat door de SAA van de Commissie wordt gecoördineerd.

25.3.3. *De Infosec-autoriteit (IA)*

Het hoofd van de Infosec-eenheid van ►**M2** het directoraat Veiligheid van de Commissie ◄ is de Infosec-autoriteit voor de Commissie. De Infosec-autoriteit heeft de volgende taken:

— technisch advies en technische bijstand verlenen aan de SAA;

— de ontwikkeling van de SSRS ondersteunen;

▼B

— de SSRS toetsen om ervoor te zorgen dat deze spoort met de onderhavige beveiligingsvoorschriften en documenten over het Infosec-beleid en de Infosec-architectuur;

— in voorkomend geval deelnemen aan accreditatiecommissies/-organen en aan de SAA accreditatie-aanbevelingen doen op het gebied van Infosec;

— Infosec-opleiding en -scholing ondersteunen;

— technisch advies geven bij onderzoeken naar Infosec-gerelateerde incidenten;

— technische richtsnoeren vaststellen om ervoor te zorgen dat alleen erkende software wordt gebruikt.

25.3.4. *Eigenaar technisch systeem (TSO)*

De verantwoordelijkheid voor de invoering en toepassing van controles en bijzondere beveiligingsvoorzieningen van een systeem ligt bij de eigenaar van dat systeem, de Eigenaar technisch systeem (TSO). Voor centraal bestuurde systemen wordt een centrale informatiebeveiligingsfunctionaris (CISO) aangewezen. Elke afdeling moet, naar gelang van het geval, een plaatselijke informatiebeveiligingsfunctionaris (LISO) aanwijzen. De TSO heeft ook tot taak operationele beveiligingsprocedures (SecOP's) te creëren en is voor het systeem verantwoordelijk gedurende zijn hele bestaan, d.w.z. van de conceptfase tot de definitieve verwijdering.

De TSO specificeert de beveiligingsnormen en -praktijken waaraan de leverancier van het systeem moet voldoen.

De TSO mag, voorzover mogelijk, een deel van zijn taken delegeren aan een plaatselijke informatiebeveiligingsfunctionaris. Eén enkele persoon kan de verschillende taken met betrekking tot INFOSEC uitvoeren.

25.3.5. *De Informatie-eigenaar (IO)*

De Informatie-eigenaar (IO) is verantwoordelijk voor EUCI (en andere informatie) die moet worden ingevoerd, verwerkt en opgesteld in technische systemen. Hij bepaalt op welke voorwaarden toegang kan worden verkregen tot de informatie in de systemen. Hij kan deze verantwoordelijkheid delegeren aan een Informatiebeheerder of een Databankbeheerder in zijn domein.

25.3.6. *Gebruikers*

De gebruikers moeten ervoor waken dat hun handelingen de beveiliging van het systeem dat zij gebruiken, niet nadelig beïnvloeden.

25.3.7. *Infosec-opleiding*

Opleiding en scholing inzake Infosec moet voor alle personeelsleden die dat nodig hebben, beschikbaar zijn.

25.4. **Niet-technische beveiligingsmaatregelen**

25.4.1. *Personeelsgerelateerde beveiliging*

Alnaargelang de rubricering en de inhoud van de gegevens die in hun specifieke systeem worden verwerkt, ondergaan gebruikers van het systeem een veiligheidsonderzoek en hebben zij een „need-to-know”. Voor toegang tot bepaalde apparatuur of gegevens in verband met de beveiliging van systemen is een bijzondere machtiging vereist, die overeenkomstig de procedures van de Commissie wordt afgegeven.

De SAA inventariseert alle gevoelige ambten en specificeert de machtigingsgraad van en het vereiste toezicht op het personeel dat die ambten bekleedt.

Het specificeren en ontwerpen van systemen gebeurt zodanig dat gemakkelijker taken en verantwoordelijkheden aan het personeel kunnen worden toegewezen zodat wordt voorkomen dat één enkele persoon volledig op de hoogte zou zijn van of controle hebben over de sleutelpunten van het systeem.

▼B

IT-zones en afzonderlijke zones met terminals/werkstations waar de beveiliging van het systeem kan worden gewijzigd, mogen niet worden bemand door slechts één gemachtigde functionaris of ander personeelslid.

De beveiligingsinstellingen van een systeem mogen alleen worden gewijzigd door twee bevoegde personeelsleden die in onderling overleg handelen.

25.4.2. *Fysieke beveiliging*

IT-zones en afzonderlijke zones met terminals/werkstations (zoals omschreven in 25.2) waar als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens met IT-middelen worden verwerkt, dan wel waar eventuele toegang tot zulke gegevens mogelijk is, dienen te worden ingericht als een EU-beveiligingszone van, naar gelang van het geval, klasse I of II.

25.4.3. *Controle op de toegang tot een systeem*

Gegevens en materiaal waarmee controle op de toegang tot een systeem mogelijk is, worden beschermd op grond van regelingen die sporen met de hoogste rubricering en de categoriebenaming van de gegevens waartoe zij toegang geven.

Indien gegevens en het materiaal voor toegangscontrole niet langer voor dat doel worden gebruikt, worden zij vernietigd overeenkomstig de voorschriften in 25.5.4.

25.5. **Technische beveiligingsmaatregelen**

25.5.1. *Beveiliging van informatie*

De opsteller van de gegevens heeft de taak om alle gegevensdragende documenten — zowel in de vorm van een niet-elektronische output als in de vorm van een digitaal opslagmedium — te identificeren en te rubriceren. Elke bladzijde van een niet-elektronische output wordt boven- en onderaan gemarkeerd met de betreffende rubricering. Een output - zowel in niet-elektronische vorm als in de vorm van een digitaal opslagmedium - heeft dezelfde rubricering als de hoogste rubricering van de gegevens die voor de vervaardiging ervan zijn gebruikt. De wijze waarop een systeem functioneert, kan eveneens gevolgen hebben voor de rubricering van outputs van dat systeem.

De diensten van de Commissie en de houders van hun gegevens hebben tot taak om problemen met betrekking tot de samenvoeging van afzonderlijke gegevenselementen aan te pakken, en te bekijken welk voordeel uit de wisselwerking tussen gerelateerde elementen kan worden gehaald, alsmede te bepalen of al dan niet een hogere rubricering dient te worden gegeven aan het geheel van de gegevens.

Het feit dat de gegevens de vorm kunnen aannemen van een verkortingscode, een transmissiecode of een binaire weergavevorm, biedt geen beveiliging en mag bijgevolg geen weerslag hebben op de rubricering van de gegevens.

Indien gegevens van het ene systeem naar het andere worden overgedragen, worden de gegevens zowel tijdens de overdracht als in het ontvangende systeem beschermd conform de oorspronkelijke rubricering en gegevenscategorie.

Digitale opslagmedia worden behandeld conform de hoogste rubricering van de opgeslagen gegevens of het label van het betreffende medium, en worden te allen tijde afdoende beschermd.

Herbruikbare digitale opslagmedia die gebruikt zijn om gerubriceerde EU-gegevens vast te leggen, behouden de hoogste rubriceringsgraad waarvoor zij ooit zijn gebruikt, totdat de gegevens een lagere rubricering hebben gekregen c.q. zijn gederubriceerd en die media dienovereenkomstig zijn geherrubriceerd, dan wel een lagere rubricering hebben gekregen of overeenkomstig een door de SAA goedgekeurde procedure vernietigd zijn (zie 25.5.4).

▼B

25.5.2. *Controle van en verantwoordelijkheid voor gegevens*

De toegang tot als ►M1 SECRET UE ◄ en hoger gerubriceerde gegevens wordt vastgelegd in automatische („audit trails") of manuele logboeken. Deze toegangsregistratie wordt overeenkomstig de beveiligingsvoorschriften van de Raad bewaard.

Gerubriceerde EU-outputs die in de IT-zone worden bewaard, mogen als gerubriceerd materiaal worden behandeld en hoeven niet te worden geregistreerd, mits het materiaal is geïdentificeerd, met de desbetreffende rubricering is gemarkeerd en afdoende wordt gecontroleerd.

Indien outputs van een systeem waarin gerubriceerde EU-gegevens worden verwerkt, van een IT-zone overgedragen worden naar een zone met afzonderlijke terminals/werkstations, worden door de SAA goed te keuren procedures voor de controle en registratie van die outputs vastgesteld. Voor de rubricering ►M1 SECRET UE ◄ en hoger omvatten zulke procedures specifieke instructies met betrekking tot de verantwoordelijkheid voor de gegevens.

25.5.3. *Behandeling en controle van verwijderbare digitale opslagmedia*

Als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde verwijderbare digitale opslagmedia worden als materiaal behandeld en vallen onder de toepassing van de algemene regels. De desbetreffende identificatie- en rubriceringsmarkeringen dienen te worden aangepast aan de specifieke fysieke verschijningsvormen van de media, zodat deze duidelijk kunnen worden herkend.

Het is aan de gebruikers om ervoor te zorgen dat gerubriceerde EU-gegevens met de juiste rubriceringsmarkering en bescherming op de betreffende media worden opgeslagen. Er dienen procedures te worden vastgelegd om er voor alle graden van EU-gegevens voor te zorgen dat de gegevens conform de beveiligingsvoorschriften op digitale opslagmedia worden opgeslagen.

25.5.4. *Derubricering en vernietiging van digitale opslagmedia*

Digitale opslagmedia die worden gebruikt om gerubriceerde EU-gegevens vast te leggen, kunnen een lagere rubricering krijgen c.q. gederubriceerd worden overeenkomstig een door de SAA goed te keuren procedure.

Digitale opslagmedia waarop als ►M1 TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens of gegevens uit bijzondere gegevenscategorieën zijn opgeslagen, mogen geen lagere rubricering krijgen, noch worden hergebruikt.

Is het niet mogelijk digitale opslagmedia een lagere rubricering te geven of opnieuw te gebruiken, dan worden deze conform de vorenvermelde procedure vernietigd.

25.5.5. *Communicatiebeveiliging*

►M2 De directeur van het directoraat Veiligheid van de Commissie ◄ is de Crypto-autoriteit.

Indien gerubriceerde EU-gegevens elektromagnetisch worden overgedragen, worden bijzondere maatregelen toegepast om het vertrouwelijke karakter, de integriteit en de beschikbaarheid van die overdracht te beschermen. De SAA bepaalt aan welke eisen de bescherming van de gegevensoverdracht tegen detectie en interceptie moet voldoen. De in een communicatiesysteem overgedragen gegevens worden beschermd op basis van eisen op het gebied van vertrouwelijke behandeling, integriteit en beschikbaarheid.

Is versleuteling vereist om het vertrouwelijke karakter, de integriteit en de beschikbaarheid te beschermen, dan worden de bedoelde methodes of aanverwante producten daartoe specifiek goedgekeurd door de SAA als Crypto-autoriteit.

▼B

Tijdens de overdracht wordt het vertrouwelijke karakter van als ►M1 SECRET UE ◄ en hoger gerubriceerde gegevens beschermd door middel van methoden of producten voor versleuteling die door de met beveiliging belaste Commissaris zijn goedgekeurd na overleg met de Adviesgroep Beveiligingsbeleid van de Commissie. Tijdens de overdracht wordt het vertrouwelijke karakter van als ►M1 CONFIDENTIEL UE ◄ of ►M1 RESTREINT UE ◄ gerubriceerde gegevens beschermd door middel van methoden of producten voor versleuteling die door de Crypto-autoriteit van de Commissie zijn goedgekeurd na overleg met de Adviesgroep Beveiligingsbeleid van de Commissie.

Gedetailleerde regels voor de overdracht van gerubriceerde EU-gegevens worden vastgelegd in specifieke beveiligingsinstructies, die door ►M2 het directoraat Veiligheid van de Commissie ◄ zijn goedgekeurd na overleg met de Adviesgroep Beveiligingsbeleid.

In uitzonderlijke operationele omstandigheden kunnen als ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ en ►M1 SECRET UE ◄ gerubriceerde gegevens in niet-versleutelde vorm worden overgedragen, voorzover de informatie-eigenaar daartoe uitdrukkelijk toestemming heeft gegeven en het geval heeft geregistreerd. Zulke uitzonderlijke omstandigheden doen zich voor:

a) in geval van een dreigende of reële crisis, een conflict of oorlogssituatie;

b) indien het van het allerhoogste belang is dat de gegevens snel ter beschikking worden gesteld en er geen versleutelingsmiddelen voorhanden zijn, en indien geoordeeld wordt dat de overgedragen gegevens niet tijdig kunnen worden misbruikt om lopende operaties te schaden.

Een systeem dient in zijn afzonderlijke werkstations of terminals over de mogelijkheid van positieve toegangsweigering tot gerubriceerde EU-gegevens te beschikken, zo nodig door fysieke scheiding dan wel door bijzondere, door de SAA goedgekeurde software.

25.5.6. *Installatie- en stralingsbeveiliging*

Met betrekking tot de basisinstallatie van systemen en elke ingrijpende wijziging daarvan zijn de specificaties zodanig dat de installatie uitgevoerd wordt door gemachtigde technici die onder permanent toezicht staan van technisch gekwalificeerd personeel dat, wat de toegang tot gerubriceerde EU-gegevens betreft, over een machtigingsgraad beschikt die overeenstemt met de hoogste rubricering van de gegevens die, naar verwachting, in het systeem zullen worden opgeslagen en verwerkt.

Systemen waarin als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde gegevens worden verwerkt, worden zodanig beschermd dat hun beveiliging niet kan worden bedreigd door compromitterende lekken; het onderzoek naar en het toezicht op zulke lekken is bekend onder de naam „Tempest”.

Anti-Tempest-maatregelen moeten worden gecontroleerd en goedgekeurd door de Tempest-autoriteit (zie 25.3.2).

25.6. **Beveiliging tijdens verwerking**

25.6.1. *Operationele beveiligingsprocedures (SecOP's)*

De operationele beveiligingsprocedures (SecOP's) bepalen de aan te nemen beveiligingsprincipes, de te volgen operationele procedures en de verantwoordelijkheden van het personeel. De SecOP's worden opgesteld onder de verantwoordelijkheid van de eigenaar technisch systeem (TSO).

25.6.2. *Bescherming van software/configuratiebeheer*

De beveiliging van de applicatieprogramma's wordt op basis van een beoordeling van de veiligheidsrubricering van het programma vastgesteld, en niet op basis van de rubricering van de gegevens die erin zullen worden verwerkt. De gebruikte softwareversies dienen regelmatig te worden getoetst op integriteit en correct functioneren.

▼B

Nieuwe of gewijzigde softwareversies mogen pas worden gebruikt om gerubriceerde EU-gegevens te verwerken nadat zij door de Eigenaar technisch systeem (TSO) zijn geverifieerd.

25.6.3. *Controle op de aanwezigheid van kwaadaardige software/computervirussen*

Er vindt regelmatig een controle op de aanwezigheid van kwaadaardige software/computervirussen plaats, overeenkomstig de door de SAA gestelde eisen.

Alle digitale opslagmedia die bij de Commissie toekomen, worden gecontroleerd op de aanwezigheid van enig kwaadaardig software- of computervirus voordat ze in het systeem worden ingevoerd.

25.6.4. *Onderhoud*

De contracten en procedures in verband met gepland onderhoud en onderhoud op afroep van systemen waarvoor een SSRS is voorgelegd, bevatten eisen en afspraken met betrekking tot het onderhoudspersoneel dat een IT-zone betreedt, en de apparatuur die het bij zich heeft.

De eisen en de procedures worden duidelijk geformuleerd in respectievelijk de SSRS en de SecOP's. Contractueel onderhoud waarbij diagnoseprocedures met toegang op afstand worden gebruikt, is alleen in uitzonderlijke omstandigheden toegestaan, onder strikte veiligheidscontrole, en vindt alleen plaats mits de SAA daarvoor haar goedkeuring verleent.

25.7. **Aankopen**

25.7.1. *Algemeen*

Elk product voor beveiliging dat met het aan te schaffen systeem zal worden gebruikt, moet ofwel reeds zijn beoordeeld en gecertificeerd, ofwel op het moment van aankoop worden beoordeeld en gecertificeerd door een bevoegde beoordelings- of certificerende instantie van één van de lidstaten van de EU, op grond van internationaal erkende criteria (zoals de Common Criteria for Information Technology Security Evaluation, ISO 15408). Om goedkeuring van de ACPC te verkrijgen zijn specifieke procedures vereist.

Bij de keuze voor de huur of de aankoop van apparatuur, en in het bijzonder van digitale opslagmedia, moet in aanmerking worden genomen dat het gebruik van dergelijke apparatuur voor de verwerking van gerubriceerde EU-gegevens inhoudt dat deze apparatuur een dienovereenkomstig beveiligde omgeving niet kan verlaten zonder eerst te zijn gederubriceerd, na goedkeuring door de SAA, alsmede dat een dergelijke derubricering niet altijd zal kunnen worden goedgekeurd.

25.7.2. *Accreditatie*

Alle SYSTEMEN waarvoor een SSRS moet worden voorgelegd voordat daarin gerubriceerde EU-gegevens kunnen worden verwerkt, worden door de SAA geaccrediteerd op basis van de informatie die is vervat in de SSRS, de SecOP's en elke andere relevante documentatie. Subsystemen en afzonderlijke terminals/werkstations worden geaccrediteerd als onderdeel van alle systemen waarmee zij zijn verbonden. Indien een systeem dient ter ondersteuning van zowel de Raad als andere organisaties, maken de Commissie en de bevoegde veiligheidsautoriteiten onderling afspraken met betrekking tot de accreditatie.

De accreditatie kan worden uitgevoerd overeenkomstig een door de SAA bepaalde accreditatiestrategie die afgestemd is op het systeem in kwestie.

25.7.3. *Beoordeling en certificatie*

Vóór accreditatie worden de beveiligingsvoorzieningen van de hardware, firmware en software van een systeem in sommige gevallen beoordeeld en gecertificeerd op de mogelijkheid om gegevens op de beoogde rubriceringsgraad te waarborgen.

De beoordelings- en certificatie-eisen worden opgenomen in de systeemplanning en duidelijk geformuleerd in de SSRS.

▼B

De beoordeling en certificatie worden uitgevoerd overeenkomstig goedgekeurde richtsnoeren door technisch gekwalificeerd en dienovereenkomstig gemachtigd personeel, namens de TSO.

De teams kunnen ter beschikking worden gesteld door een aangewezen instantie voor beoordeling of certificatie van een lidstaat of aangewezen vertegenwoordigers van die instantie, bijvoorbeeld een bevoegde en gemachtigde contractant.

De mate van beoordeling en certificatie kan worden versoepeld (bijvoorbeeld, alleen voor integratieaspecten) indien systemen gebaseerd zijn op bestaande, op nationaal niveau beoordeelde en gecertificeerde producten voor computerbeveiliging.

25.7.4. *Routinecontrole van beveiligingsvoorzieningen met het oog op verlenging van de accreditatie*

De TSO legt procedures voor routinecontroles vast, die tot doel hebben na te gaan of alle beveiligingsvoorzieningen van het systeem nog steeds geldig zijn.

In de SSRS wordt duidelijk opgesomd en verklaard welke soorten wijzigingen aanleiding geven tot heraccreditatie of vooraf door de SAA moeten worden goedgekeurd. Na elke wijziging, herstelling of storing die van invloed zou kunnen zijn geweest voor de beveiligingsvoorzieningen van het IT-systeem vergewist de TSO zich ervan dat wordt gecontroleerd of de beveiligingsvoorzieningen correct functioneren. Normaliter wordt de accreditatie van het systeem alleen verlengd als de controleresultaten bevredigend zijn.

Alle systemen met beveiligingsvoorzieningen worden regelmatig gecontroleerd of getoetst door de SAA. Wat systemen betreft waarin als ►**M1** TRES SECRET UE/EU TOP SECRET ◄ gerubriceerde gegevens worden verwerkt, worden de controles op zijn minst jaarlijks uitgevoerd.

25.8. **Tijdelijk of occasioneel gebruik**

25.8.1. *Beveiliging van microcomputers/personal computers*

Microcomputers/personal computers (PC's) met vaste schijven (of andere permanente opslagmedia) die als stand-alone of als netwerkconfiguraties worden gebruikt, alsmede draagbare computerapparatuur (bijvoorbeeld draagbare PC's en elektronische „notebooks") met vaste harde schijven worden beschouwd als media voor gegevensopslag in dezelfde zin als floppydisks of andere verwijderbare digitale opslagmedia.

Inzake toegang, verwerking, opslag en vervoer stemt de bescherming van deze apparatuur overeen met de hoogste rubriceringsgraad van gegevens die er ooit in werden verwerkt of opgeslagen (totdat die gegevens een lagere rubricering hebben gekregen c.q. overeenkomstig goedgekeurde procedures zijn gederubriceerd).

25.8.2. *Gebruik van privé IT-apparatuur voor officiële Commissiewerkzaamheden*

Het is verboden particuliere verwijderbare digitale opslagmedia, software en IT-hardware (bijvoorbeeld PC's en draagbare computerapparatuur) met opslagcapaciteit te gebruiken om gerubriceerde EU-gegevens te verwerken.

Particuliere hardware, software en media mogen alleen in een zone van klasse I of klasse II waar gerubriceerde EU-gegevens worden verwerkt, worden binnengebracht met schriftelijke toestemming van ►**M2** de directeur van het directoraat Veiligheid van de Commissie ◄. Die toestemming kan alleen in uitzonderlijke gevallen om technische redenen worden verleend.

▼B

25.8.3. *Gebruik van IT-apparatuur van een contractant of van een lidstaat voor officiële Commissiewerkzaamheden*

Het gebruik van de IT-apparatuur of software van een contractant in organisaties ter ondersteuning van officiële Commissiewerkzaamheden kan worden toegestaan door ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄. Het gebruik van nationaal ter beschikking gestelde IT-apparatuur en software kan ook worden toegestaan. In dat geval staat de IT-apparatuur onder controle van de desbetreffende inventaris van de Commissie. Indien de IT-apparatuur bestemd is om gerubriceerde EU-gegevens te verwerken, moet de SAA in elk van deze gevallen worden geraadpleegd, zodat terdege rekening wordt gehouden met en uitvoering wordt gegeven aan de INFOSEC-aspecten die op het gebruik van die apparatuur van toepassing zijn.

26. VRIJGAVE VAN GERUBRICEERDE EU–GEGEVENS AAN DERDE LANDEN OF INTERNATIONALE ORGANISATIES

26.1.1. *Principes van de vrijgave van gerubriceerde EU-gegevens*

De Commissie als college neemt een besluit over de vrijgave van gerubriceerde EU-gegevens aan derde staten of internationale organisaties op basis van:

— soort en inhoud van dergelijke informatie;

— „need-to-know” van de ontvangers;

— de voordelen voor de EU.

De instantie waarvan de vrij te geven gerubriceerde EU-gegevens afkomstig zijn, wordt verzocht in te stemmen met vrijgave.

Dergelijke beslissingen worden geval per geval genomen afhankelijk van:

— de gewenste mate van samenwerking met de betrokken derde staten of internationale organisaties;

— het vertrouwen dat in deze staten of organisaties kan worden gesteld, hetgeen voortvloeit uit het beveiligingsniveau dat zij op de aan hen toevertrouwde gerubriceerde EU-gegevens zouden toepassen en uit de mate van overeenstemming tussen de daar en de in de EU toegepaste veiligheidsvoorschriften; de adviesgroep Veiligheidsbeleid van de Commissie zal de Commissie hierover zijn technisch advies geven.

Indien derde staten of internationale organisaties gerubriceerde EU-gegevens aanvaarden, impliceert dit de garantie dat deze de gegevens niet voor andere doeleinden gebruiken dan die welke ten grondslag aan de vrijgave of uitwisseling ervan lagen en dat zij de door de Commissie vereiste bescherming zullen bieden.

26.1.2. *Graden*

Wanneer de Commissie besloten heeft dat gerubriceerde gegevens kunnen worden vrijgegeven aan of uitgewisseld met een bepaalde staat of internationale organisatie, neemt hij een besluit over de graad van samenwerking die mogelijk is. Deze hangt met name af van het beleid en de voorschriften inzake veiligheid die de bewuste staat of organisatie toepast.

Er zijn drie graden van samenwerking:

Graad 1

Samenwerking met derde staten of internationale organisaties waarvan het beleid en de voorschriften inzake veiligheid die van de EU in hoge mate benaderen.

Graad 2

Samenwerking met derde staten of internationale organisaties waarvan het beleid en de voorschriften inzake veiligheid aanzienlijk verschillen van die van de EU.

▼B

Graad 3

Incidentele samenwerking met derde staten of internationale organisaties waarvan het beleid en de voorschriften inzake veiligheid niet kunnen worden beoordeeld.

De samenwerkingsgraad is bepalend voor de veiligheidsprocedures en -voorschriften, die nader worden omschreven in de aanhangsels 3, 4 en 5.

26.1.3. *Veiligheidsovereenkomsten*

Wanneer de Commissie besloten heeft dat er permanent of langdurig behoefte is aan de uitwisseling van gerubriceerde gegevens tussen de Commissie en derde staten of internationale organisaties, stelt hij met deze staten of organisaties overeenkomsten op inzake beveiligingsprocedures voor de uitwisseling van gerubriceerde gegevens, waarin het doel van de samenwerking en de wederzijdse voorschriften voor de bescherming van de uitgewisselde gegevens worden omschreven.

In geval van occasionele derdegraadssamenwerking, die per definitie in tijd en qua doel beperkt is, kan in plaats van voor een overeenkomst inzake beveiligingsprocedures voor de uitwisseling van gerubriceerde gegevens gekozen worden voor een eenvoudig memorandum van overeenstemming, waarin de aard van de uit te wisselen gerubriceerde gegevens en de wederzijdse verplichtingen met betrekking tot die gegevens worden omschreven, mits die gegevens niet hoger zijn gerubriceerd dan ►M1 RESTREINT UE ◄.

Ontwerpovereenkomsten inzake beveiligingsprocedures of memoranda van overeenstemming worden door ►M2 het directoraat Veiligheid van de Commissie ◄ goedgekeurd voordat zij ter aanneming aan de Commissie worden voorgelegd.

De met veiligheidszaken belaste Commissaris vraagt van de NSA's van de lidstaten alle vereiste bijstand om ervoor te zorgen dat de vrij te geven gegevens gebruikt en beschermd worden in overeenstemming met de bepalingen van de overeenkomsten inzake beveiligingsprocedures of de memoranda van overeenstemming.

▼M3

27. GEMEENSCHAPPELIJKE MINIMUMNORMEN VOOR INDUSTRIËLE VEILIGHEID

27.1. **Inleiding**

Deze afdeling behandelt de beveiligingsaspecten van industriële activiteiten die specifiek verband houden met de onderhandelingen over en het plaatsen van opdrachten of gunnen van subsidieovereenkomsten voor taken die betrekking hebben op gerubriceerde EU-gegevens of voor taken die dergelijke gegevens noodzakelijk maken en/of bevatten, alsmede de uitvoering daarvan door industriële of andere entiteiten, met inbegrip van de vrijgave van en toegang tot gerubriceerde EU-gegevens tijdens procedures voor het plaatsen van een overheidsopdracht en de oproep tot het indienen van voorstellen (aanbestedingstermijn en aan het sluiten van een overeenkomst voorafgaande onderhandelingen).

27.2. **Definities**

Voor de toepassing van deze gemeenschappelijke minimumnormen wordt verstaan onder:

a) „gerubriceerde opdracht”: een opdracht of subsidieovereenkomst voor de levering van goederen, de uitvoering van werken, de beschikbaarstelling van gebouwen of verrichting van diensten waarvan de uitvoering toegang tot of opstelling van gerubriceerde EU-gegevens vereist of behelst;

b) „gerubriceerde onderaanneming”: een overeenkomst tussen een contractant of begunstigde van een subsidie en een andere contractant (onderaannemer) voor de levering van goederen, de uitvoering van werken, de beschikbaarstelling van gebouwen of verrichting van diensten waarvan de uitvoering toegang tot of opstelling van gerubriceerde EU-gegevens vereist of behelst;

c) „contractant”: een bedrijf of juridische entiteit, in rechte bekwaam om overeenkomsten te sluiten of de begunstigde te zijn van een subsidie;

▼**M3**

d) „aangewezen veiligheidsinstantie”: een autoriteit onder het gezag van de nationale veiligheidsinstantie van een EU-lidstaat die tot taak heeft industriële of andere entiteiten te informeren over alle aspecten van het nationaal beleid inzake industriële veiligheid en leiding en bijstand te verlenen bij de uitvoering ervan. De nationale veiligheidsinstantie kan de rol van aangewezen veiligheidsinstantie op zich nemen;

e) „veiligheidsmachtiging voor een vestiging”: een administratieve beslissing van een nationale veiligheidsinstantie/aangewezen veiligheidsinstantie waaruit blijkt dat de vestiging vanuit veiligheidsoogpunt afdoende bescherming biedt voor de beveiliging van gerubriceerde EU-gegevens met een bepaalde rubriceringsgraad, en dat alle personeelsleden die toegang tot gerubriceerde EU-gegevens moeten hebben, een passend veiligheidsonderzoek hebben ondergaan en informatie hebben ontvangen over de noodzakelijke beveiligingseisen met betrekking tot de toegang tot en bescherming van gerubriceerde EU-gegevens;

f) „industriële of andere entiteit”: een contractant of onderaannemer die betrokken is bij de levering van goederen, de uitvoering van werkzaamheden of verrichting van diensten; het kan hierbij gaan om entiteiten die actief zijn op het gebied van industrie, handel, diensten, wetenschappen, onderzoek, onderwijs of ontwikkeling;

g) „industriële veiligheid”: de toepassing van beschermingsmaatregelen en -procedures om verlies of compromittering te voorkomen, op te sporen of te herstellen van gerubriceerde EU-gegevens die vóór of tijdens onderhandelingen over overeenkomsten door een contractant of onderaannemer worden verwerkt, en in het kader van gerubriceerde opdrachten;

h) „nationale veiligheidsinstantie”: de overheidsinstantie van een EU-lidstaat die de eindverantwoordelijkheid draagt voor de bescherming van gerubriceerde EU-gegevens in die lidstaat;

i) „algehele rubriceringsgraad van een opdracht”: de vaststelling van de rubriceringsgraad van de gehele opdracht of subsidieovereenkomst, gebaseerd op de rubricering van de informatie die en/of het materiaal dat in een bepaald onderdeel van de gehele opdracht of subsidieovereenkomst wordt of dient te worden opgesteld, vrijgegeven of geraadpleegd. De algehele rubriceringsgraad van een opdracht mag niet lager zijn dan de hoogste rubricering van een onderdeel ervan, maar kan hoger zijn ten gevolge van de samenvoeging;

j) „memorandum over de beveiligingsaspecten”: een geheel van bijzondere, door de aanbestedende instantie uitgevaardigde, contractvoorwaarden die een integrerend deel vormen van een gerubriceerde opdracht die de toegang tot of opstelling van gerubriceerde EU-gegevens behelst, en waarin de beveiligingseisen of de onderdelen van de opdracht die beveiligd moeten worden, worden genoemd;

k) „gids voor beveiligingsrubricering”: een document waarin wordt bepaald welke onderdelen van een programma, opdracht of subsidieovereenkomst gerubriceerd zijn en wat de toepasselijke rubriceringsgraden zijn. De gids voor beveiligingsrubricering kan gedurende de looptijd van het programma, de opdracht of de subsidieovereenkomst worden uitgebreid en gegevens kunnen geherrubriceerd worden of een lagere rubricering krijgen. De gids voor beveiligingsrubricering is een onderdeel van het memorandum over de beveiligingsaspecten.

27.3. **Organisatie**

a) De Commissie kan bij industriële of andere in een lidstaat ingeschreven entiteiten gerubriceerde opdrachten plaatsen voor taken die betrekking hebben op gerubriceerde EU-gegevens of voor taken die dergelijke gegevens noodzakelijk maken en/of bevatten.

b) Wanneer de Commissie gerubriceerde opdrachten plaatst, zorgt zij ervoor dat aan alle eisen die uit deze minimumnormen voortvloeien, wordt voldaan.

c) De Commissie werkt nauw samen met de nationale veiligheidsinstantie(s) om deze minimumnormen toe te passen op het gebied van de industriële veiligheid. De nationale veiligheidsinstanties kunnen deze taken overdragen aan een of meer aangewezen veiligheidsinstanties.

▼M3

d) De eindverantwoordelijkheid voor de bescherming van gerubriceerde EU-gegevens in industriële of andere entiteiten berust bij het bestuur van die entiteiten.

e) Iedere gerubriceerde opdracht of onderaanneming die binnen het toepassingsgebied van deze minimumnormen valt, wordt door de Commissie en/of de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie, naargelang het geval, onmiddellijk gemeld aan de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de lidstaat waar de contractant of onderaannemer is ingeschreven.

27.4. **Besluiten betreffende gerubriceerde opdrachten en subsidieovereenkomsten**

a) Bij de beveiligingsrubricering van gerubriceerde opdrachten of subsidieovereenkomsten wordt rekening gehouden met de volgende beginselen:

— de Commissie bepaalt, naargelang het geval, welke aspecten van de gerubriceerde opdracht bescherming behoeven en stelt op grond hiervan de rubriceringsgraad vast. Daarbij moet zij rekening houden met de oorspronkelijke rubriceringsgraad die door de opsteller is toegekend aan de gegevens die vóór het plaatsen van de gerubriceerde opdracht gegenereerd zijn,

— de algehele rubriceringsgraad van de opdracht mag niet lager zijn dan de hoogste rubricering van een onderdeel ervan,

— gerubriceerde EU-gegevens die op grond van contractuele activiteiten zijn gegenereerd, worden gerubriceerd overeenkomstig de gids voor beveiligingsrubricering,

— in voorkomend geval is het de taak van de Commissie de algehele rubriceringsgraad van de opdracht of de rubriceringsgraad van één van de onderdelen ervan, in overleg met de opsteller, te wijzigen en alle betrokkenen daarvan op de hoogte te stellen,

— gerubriceerde gegevens die aan de contractant of onderaannemer worden vrijgegeven of die op grond van de contractuele activiteiten worden gegenereerd, mogen niet voor andere doeleinden worden gebruikt dan die welke in de gerubriceerde opdracht zijn omschreven en mogen niet aan derden worden vrijgegeven zonder de voorafgaande schriftelijke toestemming van de opsteller.

b) De Commissie en de nationale veiligheidsinstanties/aangewezen veiligheidsinstanties van de lidstaten zorgen ervoor dat contractanten en onderaannemers bij wie een gerubriceerde opdracht wordt geplaatst die verband houdt met als CONFIDENTIEL UE of hoger gerubriceerde gegevens, alle dienstige maatregelen nemen ter bescherming van de gerubriceerde EU-gegevens die aan hen worden vrijgegeven of door hen worden gegenereerd bij de uitvoering van de gerubriceerde opdracht, in overeenstemming met hun nationale wetten en voorschriften. Niet-naleving van de beveiligingsvoorschriften kan tot beëindiging van de gerubriceerde opdracht leiden.

c) Alle industriële of andere entiteiten die betrokken zijn bij gerubriceerde opdrachten die inhouden dat als CONFIDENTIEL UE of hoger gerubriceerde gegevens worden geraadpleegd, moeten over een nationale veiligheidsmachtiging voor een vestiging beschikken. De veiligheidsmachtiging voor een vestiging wordt verleend door de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de lidstaat om te bevestigen dat de vestiging de adequate beveiliging van gerubriceerde EU-gegevens in de betreffende rubriceringsgraad kan verlenen en waarborgen.

d) Wanneer een gerubriceerde opdracht wordt geplaatst, is de veiligheidsfunctionaris voor de vestiging, die is benoemd door het management van de contractant of onderaannemer, verantwoordelijk voor het aanvragen van een veiligheidsmachtiging voor het personeel van de in die lidstaat geregistreerde industriële of andere entiteit dat gezien zijn taken in het kader van een gerubriceerde opdracht toegang moet hebben tot als CONFIDENTIEL UE of hoger gerubriceerde EU-gegevens; die veiligheidsmachtiging wordt door de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de betreffende lidstaat verleend overeenkomstig de nationale voorschriften.

▼**M3**

e) Gerubriceerde opdrachten moeten een memorandum over de beveiligingsaspecten omvatten, als gedefinieerd in afdeling 27.2, onder j). Het memorandum over de beveiligingsaspecten moet een gids voor beveiligingsrubricering omvatten.

f) Vóór het begin van een onderhandelingsprocedure over een gerubriceerde opdracht neemt de Commissie contact op met de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de lidstaat waar de betrokken industriële of andere entiteiten geregistreerd zijn, om bevestigd te krijgen dat deze houder zijn van een geldige veiligheidsmachtiging voor een vestiging; deze moet dezelfde rubriceringsgraad hebben als de opdracht.

g) De aanbestedende instantie mag geen gerubriceerde opdracht plaatsen bij een geselecteerde inschrijver voordat deze een geldige veiligheidsmachtiging voor een vestiging heeft ontvangen.

h) Behoudens andersluidende bepaling in de nationale wetgeving en voorschriften van de lidstaten, is een veiligheidsmachtiging voor een vestiging niet vereist voor opdrachten die betrekking hebben op als RESTREINT UE gerubriceerde gegevens.

i) Aanbestedingen voor gerubriceerde opdrachten moeten de bepaling omvatten dat inschrijvers die geen offerte indienen of die niet worden geselecteerd, alle documenten binnen een bepaalde termijn moeten terugzenden.

j) Het kan in bepaalde gevallen nodig zijn dat een contractant op diverse niveaus met onderaannemers onderhandelt over gerubriceerde onderaanneming. Het is de verantwoordelijkheid van de contractant ervoor te zorgen dat alle onderaannemingsactiviteiten plaatsvinden overeenkomstig de gemeenschappelijke minimumnormen die in deze afdeling zijn vervat. De contractant mag evenwel geen gerubriceerde EU-gegevens of gerubriceerd EU-materiaal doorgeven aan een onderaannemer zonder schriftelijke toestemming van de verstrekker ervan.

k) De voorwaarden waaronder een contractant een beroep kan doen op onderaannemers moeten worden omschreven in de aanbesteding of oproep tot het indienen van inschrijvingen en in de gerubriceerde opdracht. Entiteiten die geregistreerd zijn in landen die geen lidstaat van de EU zijn, mogen niet als onderaannemer worden ingeschakeld zonder de uitdrukkelijke schriftelijke toestemming van de Commissie.

l) Tijdens de gehele looptijd van de gerubriceerde opdracht ziet de Commissie, samen met nationale veiligheidsinstantie/aangewezen veiligheidsinstantie, toe op de naleving van alle beveiligingsbepalingen. Beveiligingsincidenten moeten, overeenkomstig de bepalingen van deel II, afdeling 24, van deze veiligheidsvoorschriften, worden gemeld. De wijziging of intrekking van een veiligheidsmachtiging voor een vestiging moet onmiddellijk worden gemeld aan de Commissie en aan alle nationale veiligheidsinstanties/aangewezen veiligheidsinstanties die van het bestaan ervan in kennis waren gesteld.

m) De Commissie en/of de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie, naargelang het geval, meldt de beëindiging van een gerubriceerde opdracht of gerubriceerde onderaanneming onmiddellijk bij de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de lidstaat waar de contractant of onderaannemer is geregistreerd.

n) Contractanten en onderaannemers dienen de in deze afdeling opgenomen gemeenschappelijke minimumnormen in acht te blijven nemen en de vertrouwelijkheid van gerubriceerde gegevens te blijven verzekeren, ook na beëindiging of voltooiing van de gerubriceerde opdracht of de gerubriceerde onderaanneming.

o) Specifieke bepalingen over de verwijdering van gerubriceerde gegevens na beëindiging van de gerubriceerde opdracht worden opgenomen in het memorandum over de beveiligingsaspecten of andere relevante bepalingen waarin de beveiligingseisen worden vastgesteld.

p) De in deze afdeling genoemde verplichtingen en voorwaarden zijn van overeenkomstige toepassing op de procedures waarbij subsidies bij besluit worden toegekend en met name op de begunstigden van die subsidies. In het besluit tot toekenning van de subsidie worden alle verplichtingen van de begunstigden opgesomd.

▼M3

27.5. **Bezoeken**

Bezoeken van personeelsleden van de Commissie aan industriële of andere entiteiten in de lidstaten die gerubriceerde EU-opdrachten uitvoeren, moeten met de bevoegde nationale veiligheidsinstantie/aangewezen veiligheidsinstantie worden overeengekomen. Bezoeken van werknemers van industriële of andere entiteiten in het kader van een gerubriceerde EU-opdracht moeten worden overeengekomen tussen de betrokken nationale veiligheidsinstanties/aangewezen veiligheidsinstanties. De nationale veiligheidsinstanties/aangewezen veiligheidsinstanties die betrokken zijn bij een gerubriceerde EU-opdracht, kunnen evenwel een procedure overeenkomen waarmee bezoeken van werknemers van industriële of andere entiteiten rechtstreeks kunnen worden geregeld.

27.6. **Overdracht en vervoer van gerubriceerde EU-gegevens**

a) Op de overdracht van gerubriceerde EU-gegevens zijn de bepalingen van deel II, afdeling 21, van deze veiligheidsvoorschriften van toepassing. Ter aanvulling van die bepalingen gelden de bestaande procedures die van toepassing zijn tussen de lidstaten.

b) Het internationaal vervoer van gerubriceerd EU-materiaal dat betrekking heeft op gerubriceerde opdrachten, geschiedt in overeenstemming met de nationale procedures van de lidstaten. De volgende beginselen worden toegepast bij de beoordeling van de regelingen voor de beveiliging van internationaal vervoer:

   — de beveiliging wordt in alle fasen van het vervoer en onder alle omstandigheden gewaarborgd, van het punt van oorsprong tot de eindbestemming,

   — de mate van bescherming die aan een zending wordt verleend, wordt bepaald door de hoogste rubriceringsgraad van het materiaal dat zij bevat,

   — in voorkomend geval wordt een veiligheidsmachtiging voor een vestiging aangevraagd voor de bedrijven die het vervoer verzorgen. In dat geval moeten de personeelsleden die de zending behandelen, in overeenstemming met de in deze afdeling vervatte gemeenschappelijke minimumnormen, een veiligheidsonderzoek ondergaan,

   — de reizen geschieden zoveel mogelijk zonder onderbreking en worden zo snel uitgevoerd als de omstandigheden toelaten,

   — waar mogelijk leiden de routes alleen door EU-lidstaten. Routes door niet-EU-lidstaten mogen alleen worden gevolgd met de toestemming van de nationale veiligheidsinstantie/aangewezen veiligheidsinstantie van de staat van de verzender en de staat van de geadresseerde,

   — vóór iedere verplaatsing van gerubriceerd EU-materiaal stelt de verzender een vervoerplan op, dat moet worden goedgekeurd door de betrokken nationale veiligheidsinstanties/aangewezen veiligheidsinstanties.

▼M1

Aanhangsel 1

VERGELIJKING VAN DE NATIONALE RUBRICERINGEN

EU-rubricering	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
WEU-rubricering	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratom-rubricering	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
NAVO-rubricering	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Oostenrijk	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
België	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Cyprus	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Tsjechië	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denemarken	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Duitsland	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Griekenland	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Frankrijk	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	

▼M4

Kroatië	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Ierland	Top Secret	Secret	Confidential	Restricted
Italië	Segretissimo	Segreto	Riservatissimo	Riservato
Letland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litouwen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼**M1**

Hongarije	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederland	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaal-vertrouwelijk
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Slovenië	Strogo tajno	Tajno	Zaupno	SVN Interno
Slowakije	Prísne tajné	Tajné	Dôverné	Vyhradené
Spanje	Secreto	Reservado	Confidencial	Difusión Limitada
Zweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Verenigd Koninkrijk	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) De rubricering „Très Secret Défense”, die gebruikt wordt voor belangrijke dossiers van de regering, mag slechts worden gewijzigd met toestemming van de eerste minister.
([3]) Stg = staatsgeheim.

▼B

Aanhangsel 2

PRAKTISCHE RUBRICERINGSGIDS

Deze gids is indicatief en mag niet geïnterpreteerd worden als wijziging van de inhoudelijke bepalingen van de afdelingen 16, 17, 20 en 21.

Rubricering	Wanneer	Wie	Aanbrengen rubricering	Lagere rubricering/derubricering/vernietiging	
				Wie	Wanneer
►**M1** TRES SECRET UE/EU TOP SECRET ◄: Deze rubricering wordt alleen toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging uitzonderlijk nadelig zou kunnen zijn voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten [16.1]	Indien het compromitteren van als ►**M1** TRES SECRET UE/EU TOP SECRET ◄ gerubriceerd materiaal: — een rechtstreekse bedreiging zou kunnen vormen voor de interne stabiliteit van de EU of een van haar lidstaten of bevriende landen — buitengewoon ernstige schade zou kunnen toebrengen aan de betrekkingen met bevriende regeringen — rechtstreeks zou kunnen leiden tot grote aantallen dodelijke slachtoffers — buitengewoon ernstige schade zou kunnen toebrengen aan de operationele doeltreffendheid of veiligheid van de strijdkrachten van de lidstaten of van andere contribuenten of aan de continue doeltreffendheid van uiterst waardevolle veiligheids- of inlichtingenoperaties — voor langere termijn ernstige schade zou kunnen toebrengen aan de economie van de EU of haar lidstaten.	Naar behoren gemachtigde personen (opstellers), directeuren-generaal, diensthoofden [17.1]. Opstellers vermelden op gerubriceerde documenten een datum waarop, een periode waarna of een gebeurtenis waarbij de inhoud lager gerubriceerd of gederubriceerd kan worden [16.2]. Zo niet verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkelijke rubricering moet worden gehandhaafd [17.3].	De rubricering ►**M1** TRES SECRET UE/EU TOP SECRET ◄ wordt aangebracht op ►**M1** TRES SECRET UE/EU TOP SECRET ◄- documenten; waar van toepassing wordt een beveiligingsindicator en/of de defensiemarkering ESDP mechanisch en handmatig aangebracht [16.4, 16.5, 16.3]. De EU-rubriceringen en beveiligingsindicatoren worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum; dit referentienummer wordt op elke bladzijde aangebracht. Indien er verscheidene kopieën verspreid moeten worden, krijgt elke kopie een kopienummer, dat, met het totaal aantal bladzijden, op de eerste bladzijde wordt aangebracht. Alle bijlagen en bijvoegsels worden op de eerste bladzijde vermeld [21.1].	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, welke de daaropvolgende geadresseerden aan wie hij het document heeft gezonden of voor wie hij het heeft gekopieerd, van de wijziging op de hoogte brengt [17.3]. ►**M1** TRES SECRET UE/EU TOP SECRET ◄- documenten mogen alleen vernietigd worden door het centrale of subregister dat voor die documenten verantwoordelijk is. Elk vernietigd document wordt genoteerd in een proces-verbaal van vernietiging dat ondertekend wordt door de ►**M1** TRES SECRET UE/EU TOP SECRET ◄-controlefunctionaris en de functionaris die getuige is bij de vernietiging en voor de ►**M1** TRES SECRET UE/EU TOP SECRET ◄-graad gemachtigd is. Hiervan wordt aantekening gemaakt in het logboek. Het register moet de processen-verbaal van vernietiging samen met de verspreidingsformulieren gedurende tien jaar bewaren [22.5].	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd [22.5]. ►**M1** TRES SECRET UE/EU TOP SECRET ◄-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van ►**M1** TRES SECRET UE/EU TOP SECRET ◄-documenten, zoals kladversies, ontwerpteksten, getypte aantekeningen en carbonpapier, worden onder toezicht van een ►**M1** TRES SECRET UE/EU TOP SECRET ◄-controlefunctionaris vernietigd door verbranding, verpulping, versnippering of een andere methode waardoor de documenten onherkenbaar en onherstelbaar vernietigd worden [22.5].

Rubricering	Wanneer	Wie	Aanbrengen rubricering	Lagere rubricering/derubricering/vernietiging	
				Wie	Wanneer
►M1 SECRET UE ◄: Deze rubricering wordt alleen toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging ernstige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten [16.1].	Indien het compromitteren van als ►M1 SECRET UE ◄ gerubriceerd materiaal: — internationale spanningen zou doen kunnen ontstaan — ernstige schade zou kunnen berokkenen aan de betrekkingen met vriendschappelijke regeringen — rechtstreeks levensgevaar of ernstige schade aan de openbare orde en de veiligheid of vrijheid van het individu zou kunnen veroorzaken — ernstige schade zou kunnen toebrengen aan de operationele doeltreffendheid of veiligheid van de strijdkrachten van de lidstaten of van andere contribuenten of aan de continue doeltreffendheid van uiterst waardevolle veiligheids- of inlichtingenoperaties — wezenlijke materiële schade zou kunnen berokkenen aan de EU of aan de financiële, monetaire, economische en handelsbelangen van een van haar lidstaten.	Gemachtigde personen (opstellers), directeurengeneraal, diensthoofden [17.1]. Opstellers vermelden op gerubriceerde documenten een datum waarop of een periode waarna de inhoud lager gederubriceerd of gederubriceerd kan worden [16.2]. Zo niet verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkelijke rubricering moet worden gehandhaafd [17.3].	De rubricering ►M1 SECRET UE ◄ wordt aangebracht op ►M1 SECRET UE ◄-documenten; waar van toepassing wordt een beveiligingsindicator en/of de defensiemarkering ESDP mechanisch en handmatig aangebracht [16.4, 16.5, 16.3]. De EU-rubriceringen en beveiligingsindicatoren worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum; dit referentienummer wordt op elke bladzijde aangebracht. Indien er verscheidene kopieën verspreid moeten worden, krijgt elke kopie een kopienummer, dat, met het totaal aantal bladzijden, op de eerste bladzijde wordt aangebracht. Alle bijlagen en bijvoegsels worden op de eerste bladzijde vermeld [21.1].	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, welke de daaropvolgende geadresseerden aan wie hij het document heeft gezonden of voor wie hij het heeft gekopieerd, van de wijziging op de hoogte brengt [17.3]. ►M1 SECRET UE ◄-documenten mogen alleen vernietigd worden door het register dat voor die documenten verantwoordelijk is, onder toezicht van een persoon met een veiligheidsmachtiging. Vernietigde ►M1 SECRET UE ◄-documenten worden genoteerd in een ondertekend proces-verbaal van vernietiging, dat door het register, met de verspreidingsformulieren, gedurende tenminste drie jaar bewaard wordt [22.5].	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd [22.5]. ►M1 SECRET UE ◄-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van ►M1 SECRET UE ◄-documenten, zoals kladversies, ontwerpteksten, getypte aantekeningen en carbonpapier, worden vernietigd door verbranding, verpulping, versnippering of een ander methode waardoor de documenten onherkenbaar en onherstelbaar vernietigd worden [22.5].
►M1 CONFIDENTIEL UE ◄:	Indien het compromitteren van als ►M1 CONFIDENTIEL UE ◄ gerubriceerd materiaal: — de diplomatieke betrekkingen materiële schade zou kunnen berokkenen, dat wil zeggen zou kunnen leiden tot officieel protest of andere sancties	Gemachtigde personen (opstellers), directeurengeneraal, diensthoofden [17.1].	De rubricering ►M1 CONFIDENTIEL UE ◄ wordt aangebracht op ►M1 CONFIDENTIEL UE ◄-documenten; waar van toepassing wordt een beveiligingsindicator en/of de defensiemarkering ESDP mechanisch en handmatig aangebracht, of door het drukken op voorgemerkt, geregistreerd papier [16.4, 16.5, 16.3].	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, welke de daaropvolgende geadresseerden aan wie hij het document heeft gezonden of voor wie hij het heeft gekopieerd, van de wijziging op de hoogte brengt [17.3].	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd [22.5].

▼B

Rubricering	Wanneer	Wie	Aanbrengen rubricering	Lagere rubricering/derubricering/vernietiging	
				Wie	Wanneer
Deze rubricering wordt toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten [16.1].	— de vrijheid van het individu zou kunnen schaden — schade zou kunnen toebrengen aan de operationele doeltreffendheid of veiligheid van de strijdkrachten van de lidstaten of van andere contribuenten of aan de doeltreffendheid van waardevolle veiligheids- of inlichtingenoperaties — de financiële levensvatbaarheid van belangrijke organisaties wezenlijk zou kunnen ondermijnen — het onderzoek van ernstige criminaliteit zou kunnen verhinderen of het begaan ervan zou kunnen vergemakkelijken — wezenlijk zou kunnen indruisen tegen de financiële, monetaire, economische en handelsbelangen van de EU of haar lidstaten — de ontwikkeling of werking van de voornaamste EU-beleidsvormen ernstig zou kunnen hinderen — significante activiteiten van de EU zou kunnen blokkeren of anderszins ernstig verstoren.	Opstellers vermelden op gerubriceerde documenten een datum waarop of een periode waarna de inhoud lager gederubriceerd of gederubriceerd kan worden. Zo niet verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkelijke rubricering moet worden gehandhaafd [17.3].	Die EU-rubriceringen worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk gerubriceerd EU-document krijgt een referentienummer en een datum. Alle bijlagen en bijvoegsels worden op de eerste bladzijde vermeld [21.1].	►M1 CONFIDENTIEL UE ◄-documenten mogen alleen vernietigd worden door het register dat voor die documenten verantwoordelijk is, onder toezicht van een persoon met een veiligheidsmachtiging. De vernietigde documenten worden genoteerd overeenkomstig de nationale voorschriften of, in het geval van de Commissie of gedecentraliseerde EU-organen, volgens de instructies van ►M2 het voor veiligheid bevoegde Commissielid ◄ [22.5].	►M1 CONFIDENTIEL UE ◄-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van ►M1 CONFIDENTIEL UE ◄-documenten, zoals kladversies, ontwerpteksten, getypte aantekeningen en carbonpapier, worden vernietigd door verbranding, verpulping, versnippering of een andere methode waardoor de documenten onherkenbaar en onherstelbaar vernietigd worden [22.5].

▼B

Rubricering	Wanneer	Wie	Aanbrengen rubricering	Lagere rubricering/derubricering/vernietiging	
				Wie	Wanneer
►M1 RESTREINT UE ◄: Deze rubricering wordt toegepast op gegevens en materiaal waarvan de openbaarmaking zonder machtiging nadelig zou kunnen zijn voor de belangen van de Europese Unie of van één of meer van haar lidstaten [16.1].	Indien het compromitteren van als ►M1 RESTREINT UE ◄ gerubriceerd materiaal: — nadeling zou kunnen zijn voor de diplomatieke betrekkingen — wezenlijke schade zou kunnen berokkenen aan het individu — de handhaving van de operationele doeltreffendheid of de veiligheid van de strijdkrachten van de lidstaten of van andere contribuenten zou kunnen bemoeilijken — bij personen of ondernemingen zou kunnen leiden tot financiële verliezen of oneigenlijke winsten of voordelen in de hand zou kunnen werken — bonafide ondernemingen ertoe zou kunnen aanzetten om de geheimhouding van informatie van derde partijen te schenden — statutaire beperkingen op de openbaarmaking van informatie zou kunnen schenden, — het onderzoek van criminaliteit zou kunnen schaden of het begaan ervan zou kunnen vergemakkelijken — de EU of haar lidstaten zou kunnen benadelen bij handels- of politieke onderhandelingen met andere partijen — de effectieve ontwikkeling of werking van de EU-beleidsvormen zou kunnen hinderen — een goed beheer van de EU en haar operaties zou kunnen ondermijnen.	Gemachtigde personen (opstellers), directeurengeneraal, diensthoofden [17.1]. Opstellers vermelden op gerubriceerde documenten een datum waarop, een periode waarna of een gebeurtenis waarbij de inhoud lager gerubriceerd of gederubriceerd kan worden [16.2]. Zo niet verifiëren zij de documenten uiterlijk om de vijf jaar om zich ervan te vergewissen of de oorspronkekijke rubricering moet worden gehandhaafd [17.3].	De rubricering ►M1 RESTREINT UE ◄ wordt aangebracht op ►M1 RESTREINT UE ◄-documenten; waar van toepassing wordt een beveiligingsindicator en/of de defensiemarkering ESDP mechanisch en handmatig aangebracht [16.4, 16.5, 16.3]. De EU-rubriceringen en beveiligingsindicatoren worden bovenaan op de eerste bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum [21.1].	Derubricering is de uitsluitende verantwoordelijkheid van de opsteller, welke de daaropvolgende geadresseerden, aan wie hij het document heeft gezonden of voor wie hij het heeft gekopieerd, van de wijziging op de hoogte brengt [17.3]. ►M1 RESTREINT UE ◄-documenten worden vernietigd door het register dat voor die documenten verantwoordelijk is of door de gebruiker, volgens de instructies van ►M2 het voor veiligheid bevoegde Commissielid ◄ [22.5].	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd. [22.5].

▼B

Aanhangsel 3

Richtsnoeren voor vrijgave van gerubriceerde EU-gegevens aan derde staten of internationale organisaties: eerstegraadssamenwerking

PROCEDURES

1. De bevoegdheid om gerubriceerde EU-gegevens vrij te geven aan landen die het Verdrag betreffende de Europese Unie niet hebben ondertekend of aan andere internationale organisaties waarvan het beleid en de voorschriften inzake beveiliging vergelijkbaar zijn met die van de EU, berust bij de Commissie als college.

2. In afwachting van de sluiting van een beveiligingsovereenkomst is het voor veiligheid verantwoordelijke Commissielid bevoegd om verzoeken om vrijgave van gerubriceerde EU-gegevens (EUCI) te onderzoeken.

3. Daarvoor:

   — wint hij/zij het advies in van de opstellers van de vrij te geven EUCI;

   — legt hij/zij de nodige contacten met de beveiligingsinstanties van de begunstigde staten of internationale organisaties om na te gaan of hun beleid en voorschriften inzake beveiliging garanderen dat de vrij te geven gerubriceerde gegevens in overeenstemming met deze veiligheidsvoorschriften zullen worden beschermd;

   — wint hij/zij technisch advies in bij de Adviesgroep Veiligheidsbeleid van de Commissie met betrekking tot het vertrouwen dat kan worden gesteld in de begunstigde staten of internationale organen.

4. Het voor veiligheid bevoegde Commissielid stuurt het verzoek en het advies van de Adviesgroep Veiligheidsbeleid van de Commissie door naar de Commissie, die daarover een besluit neemt.

VEILIGHEIDSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

5. Het voor veiligheid bevoegde Commissielid deelt het besluit van de Commissie om vrijgave van gerubriceerde EU-gegevens toe te staan, mee aan de begunstigde staten of internationale organisaties.

6. Het besluit houdende vrijgave treedt niet eerder in werking dan nadat de begunstigden schriftelijk hebben verzekerd dat zij:

   — de gegevens niet voor andere dan de overeengekomen doeleinden zullen gebruiken;

   — de gegevens zullen beschermen in overeenstemming met deze veiligheidsvoorschriften en meer bepaald de onderstaande bijzondere voorschriften.

7. Personeel

   a) Het aantal functionarissen dat toegang krijgt tot de gerubriceerde EU-gegevens wordt op basis van het „need-to-know”-beginsel strikt beperkt tot diegenen wier functie toegang noodzakelijk maakt.

   b) Alle functionarissen of burgers die gemachtigd zijn toegang te hebben tot als ►**M1** CONFIDENTIEL UE ◄ of hoger gerubriceerde gegevens zijn in het bezit van een veiligheidsattest van het gewenste niveau of van een daarmee gelijkwaardige veiligheidsmachtiging, die beide door de regering van hun eigen land zijn afgegeven.

8. Overdracht van documenten

   a) De praktische procedures voor de overdracht van documenten wordt geregeld in een overeenkomst. In afwachting van de sluiting van zo'n overeenkomst zijn de bepalingen van Afdeling 21 van toepassing. In de overeenkomst wordt met name gespecificeerd aan welke registers de gerubriceerde EU-gegevens worden toegestuurd.

▼B

b) Indien de gerubriceerde gegevens waarvan de Commissie de vrijgave heeft goedgekeurd ►M1 TRES SECRET UE/EU TOP SECRET ◄-gegevens bevatten, zet de begunstigde staat of internationale organisatie een centraal EU-register en zo nodig EU-subregisters op. Deze registers passen strikt dezelfde voorschriften toe als die van Afdeling 22 van deze veiligheidsvoorschriften.

9. Registratie

Zodra een register een als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerd EU-document ontvangt, wordt het document ingeschreven in een speciaal daarvoor door de organisatie aangelegd bestand met kolommen voor de datum van ontvangst, de bijzonderheden van het document (datum, referentie- en kopienummer), de rubricering, de titel, de naam en de titel van de ontvanger, de datum waarop het ontvangstbewijs is teruggestuurd en de datum waarop het document is teruggestuurd naar de broninstantie van de EU of vernietigd is.

10. Vernietiging

a) Gerubriceerde EU-documenten worden vernietigd in overeenstemming met de instructies in Afdeling 22 van deze veiligheidsvoorschriften. Kopieën van het proces-verbaal van vernietiging voor ►M1 SECRET UE ◄- en ►M1 TRES SECRET UE/EU TOP SECRET ◄-documenten worden aan het EU-register gestuurd dat de documenten heeft toegezonden.

b) Gerubriceerde EU-documenten worden opgenomen in de noodvernietigingsplannen die gelden voor de gerubriceerde documenten van de begunstigde organen zelf.

11. Bescherming van documenten

Alles wordt in het werk gesteld om te voorkomen dat onbevoegden toegang hebben tot gerubriceerde EU-gegevens.

12. Kopieën, vertalingen en uittreksels

Van een als ►M1 CONFIDENTIEL UE ◄ of ►M1 SECRET UE ◄ gerubriceerd document mogen geen fotokopieën, vertalingen of uittreksels worden gemaakt zonder toestemming van het hoofd van de beveiligingsorganisatie, die deze kopieën, vertalingen en uittreksels registreert, controleert en zo nodig afstempelt.

De reproductie of vertaling van een ►M1 TRES SECRET UE/EU TOP SECRET ◄-document kan alleen geschieden met instemming van de instantie waarvan het afkomstig is, die aangeeft hoeveel kopieën er mogen worden gemaakt; indien niet kan worden uitgemaakt van welke autoriteit het document afkomstig is, wordt het verzoek doorgegeven aan ►M2 het directoraat Veiligheid van de Commissie ◄.

13. Inbreuken op de veiligheidsvoorschriften

Wanneer een inbreuk heeft plaatsgevonden of vermoedelijk heeft plaatsgevonden met betrekking tot een gerubriceerd EU-document worden, onder voorbehoud van de sluiting van een beveiligingsovereenkomst, onmiddellijk de volgende maatregelen getroffen:

a) uitvoeren van een onderzoek naar de omstandigheden van de inbreuk;

b) informeren van ►M2 het directoraat Veiligheid van de Commissie ◄, de nationale veiligheidsinstantie en de instantie waarvan het document afkomstig is, of indien dit laatste niet is geschied, daar duidelijk melding van maken;

c) beperken van de gevolgen van de inbreuk;

d) maatregelen om herhaling te voorkomen overwegen en uitvoeren;

e) de door ►M2 het directoraat Veiligheid van de Commissie ◄ aanbevolen maatregelen om herhaling te voorkomen, uitvoeren.

▼B

14. Inspecties

►M2 Het directoraat Veiligheid van de Commissie ◄ wordt door middel van een overeenkomst met de betrokken staten of internationale organisaties gemachtigd een evaluatie uit te voeren van de doeltreffendheid van de maatregelen ter bescherming van de vrijgegeven gerubriceerde EU-gegevens.

15. Rapportage

Onder voorbehoud van de sluiting van een beveiligingsovereenkomst brengt de staat of internationale organisatie die de gerubriceerde EU-gegevens onder zich houdt jaarlijks, op een bij de instemming met de vrijgave van de gegevens gespecificeerde datum, verslag uit om te bevestigen dat deze veiligheidsvoorschriften zijn nageleefd.

▼B

Aanhangsel 4

Richtsnoeren voor vrijgave van gerubriceerde EU-gegevens aan derde staten of internationale organisaties: tweedegraadssamenwerking

PROCEDURES

1. De bevoegdheid om gerubriceerde EU-gegevens vrij te geven aan derde staten of internationale organisaties, waarvan het beleid en de voorschriften inzake beveiliging aanzienlijk verschillen van die van de EU, berust bij de opsteller. De bevoegdheid om binnen de Commissie gecreëerde EUCI vrij te geven berust bij de Commissie als college.

2. In beginsel is de bevoegdheid beperkt tot gegevens met een rubricering tot en met ►**M1** SECRET UE ◄; gerubriceerde gegevens die beschermd worden door bijzondere beveiligingsindicatoren of markeringen zijn hiervan uitgesloten.

3. In afwachting van de sluiting van een beveiligingsovereenkomst is het voor veiligheid verantwoordelijke Commissielid bevoegd om verzoeken om vrijgave van gerubriceerde EU-gegevens te onderzoeken.

4. Daarvoor:

   — wint hij/zij het advies in van de opstellers van de vrij te geven EUCI;

   — legt hij/zij eerste contacten met de beveiligingsinstanties van de begunstigde staten of internationale organisaties om informatie in te winnen over hun beleid en voorschriften inzake beveiliging, en in het bijzonder om een vergelijkende tabel op te stellen van de in de EU en in de betrokken staat of organisatie van toepassing zijnde rubriceringen;

   — belegt hij/zij een bijeenkomst van de Adviesgroep Veiligheidsbeleid van de Commissie of doet hij/zij zo nodig, volgens een stilzwijgende procedure, navraag bij de nationale veiligheidsinstanties van de lidstaten om het technisch advies van de Adviesgroep Veiligheidsbeleid van de Commissie in te winnen.

5. Het advies van de Adviesgroep Veiligheidsbeleid van de Commissie behelst:

   — het vertrouwen dat kan worden gesteld in de begunstigde staten of internationale organisaties met het oog op een evaluatie van de beveiligingsrisico's waaraan de EU of haar lidstaten blootstaan;

   — een evaluatie van het vermogen van de begunstigden om door de EU vrijgegeven gerubriceerde gegevens te beschermen;

   — voorstellen voor praktische procedures voor de verwerking van gerubriceerde EU-gegevens (bijvoorbeeld het verstrekken van gekuiste versies van een tekst) en overgedragen documenten (niet-vermelding of verwijdering van EU-rubriceringsopschriften, specifieke markeringen enz.);

   — lagere rubricering of derubricering voordat de gegevens worden vrijgegeven aan de begunstigde landen of internationale organisaties.

6. Het voor veiligheid bevoegde Commissielid stuurt het verzoek en het advies van de Adviesgroep Veiligheidsbeleid van de Commissie door naar de Commissie, die daarover een besluit neemt.

VEILIGHEIDSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

7. Het voor veiligheid bevoegde Commissielid deelt het besluit van de Commissie om vrijgave van gerubriceerde EU-gegevens toe te staan, en de daarbij geldende beperkingen, mee aan de begunstigde staten of internationale organisaties.

▼B

8. Het besluit houdende vrijgave treedt niet eerder in werking dan nadat de begunstigden schriftelijk hebben verzekerd dat zij:

   — de gegevens niet voor andere dan de overeengekomen doeleinden zullen gebruiken;

   — de gegevens zullen beschermen in overeenstemming met de veiligheidsvoorschriften van de Commissie.

9. De volgende beschermingsvoorschriften zijn van toepassing, tenzij de Commissie, na inwinning van het technisch advies van de Adviesgroep Veiligheidsbeleid van de Commissie, besluit een bijzondere procedure vast te stellen voor de verwerking van gerubriceerde EU-documenten (niet-vermelding van de EU-rubricering, specifieke markering enz.).

10. Personeel

   a) Het aantal functionarissen dat toegang krijgt tot gerubriceerde EU-gegevens wordt op basis van het „need-to-know”-beginsel strikt beperkt tot diegenen wier functie toegang noodzakelijk maakt.

   b) Alle functionarissen of burgers die gemachtigd zijn toegang te hebben tot door de Commissie vrijgegeven gerubriceerde gegevens zijn in het bezit van een nationale veiligheidsmachtiging of toegangsmachtiging, tot een passend niveau dat gelijkwaardig is aan dat van de EU zoals gedefinieerd in de vergelijkende tabel.

   c) Deze nationale veiligheidsmachtigingen of toegangsmachtigingen worden ter informatie aan ►M2 de directeur van het directoraat Veiligheid van de Commissie ◄ gestuurd.

11. Overdracht van documenten

   De praktische procedures voor de overdracht van documenten wordt geregeld in een overeenkomst. In afwachting van de sluiting van zo'n overeenkomst zijn de bepalingen van Afdeling 21 van toepassing. In de overeenkomst wordt met name gespecificeerd aan welke registers de gerubriceerde EU-gegevens worden toegestuurd; ook worden daarin de adressen vermeld waarnaar de documenten worden gestuurd, en wordt vermeld welke post- of koerierdiensten voor de overdracht van de gerubriceerde EU-gegevens worden ingeschakeld.

12. Registratie bij ontvangst

   De nationale veiligheidsinstantie van de geadresseerde staat of haar tegenhanger in de staat die namens de regering de door de Commissie toegezonden gerubriceerde gegevens ontvangt of het beveiligingsbureau van de ontvangende internationale organisatie, legt een speciaal bestand aan om bij ontvangst gerubriceerde EU-gegevens te registreren. Dit bestand omvat kolommen voor de datum van ontvangst, de bijzonderheden van het document (datum, referentie- en kopienummer), de rubricering, de titel, de naam of de titel van de geadresseerde, de datum waarop het ontvangstbewijs is teruggestuurd en de datum waarop het document is teruggestuurd naar de EU of vernietigd is.

13. Terugsturen van documenten

   Wanneer de ontvanger een gerubriceerd document terugstuurt naar de Commissie, handelt deze in overeenstemming met het bovenstaande punt „Overdracht van documenten”.

14. Bescherming

   a) Wanneer de documenten niet worden gebruikt, worden ze opgeslagen in een beveiligingsopbergmiddel dat is goedgekeurd voor de opslag van nationaal gerubriceerd materiaal van dezelfde rubriceringsgraad. Op het opbergmiddel staat geen indicatie van de inhoud, die alleen toegankelijk is voor personen die gemachtigd zijn om gerubriceerde EU-gegevens te verwerken. In geval van gebruik van combinatiesloten is de combinatie alleen bekend bij de functionarissen van de staat of organisatie die een toegangsmachtiging hebben voor de daarin opgeslagen gerubriceerde EU-gegevens; de combinatie wordt om de zes maanden gewijzigd of eerder, dit bij overplaatsing van een functionaris, bij intrekking van de veiligheidsmachtiging van een van de functionarissen die de combinatie kent of indien er een risico van compromittering is.

▼B

b) Gerubriceerde EU-documenten worden alleen uit het beveiligingsopbergmiddel genomen door functionarissen die een toegangsmachtiging hebben voor de gerubriceerde EU-documenten en die hiervan kennis moeten nemen. Zolang deze documenten in hun bezit zijn, blijven zij verantwoordelijk voor de veilige bewaring ervan, en dienen zij in het bijzonder te garanderen dat onbevoegden geen toegang krijgen tot de documenten. Ook zorgen zij ervoor dat de documenten worden opgeborgen in een beveiligingsopbergmiddel zodra zij de documenten niet meer raadplegen alsook buiten de werktijden.

c) Zonder toestemming van ►M2 het directoraat Veiligheid van de Commissie ◄ mogen er geen fotokopieën of uittreksels worden gemaakt van als ►M1 CONFIDENTIEL UE ◄ of hoger gerubriceerde documenten.

d) De procedure voor snelle en volledige vernietiging van documenten in noodgevallen wordt vastgesteld en bevestigd door ►M2 het directoraat Veiligheid van de Commissie ◄.

15. Fysieke bescherming

a) Wanneer er geen documenten in gebruik zijn dienen de beveiligingsopbergmiddelen voor gerubriceerde EU-documenten te allen tijde afgesloten te zijn.

b) Wanneer onderhouds- of schoonmaakpersoneel een ruimte dient te betreden die dergelijke opbergmiddelen bevat of wanneer het in zo'n ruimte dient te werken, wordt het personeel te allen tijde begeleid door een lid van de veiligheidsdienst van de staat of de organisatie of door de functionaris die meer in het bijzonder verantwoordelijk is voor het toezicht op de beveiliging van de ruimte.

c) Buiten normale werktijden ('s nachts, in het weekend en op feestdagen) worden de beveiligingsopbergruimten die gerubriceerde EU-documenten bevatten beschermd door een bewaker of een automatisch alarmsysteem.

16. Inbreuken op de veiligheidsvoorschriften

Wanneer er in verband met gerubriceerde EU-gegevens een inbreuk heeft plaatsgevonden of vermoedelijk heeft plaatsgevonden, worden onmiddellijk de volgende maatregelen getroffen:

a) onmiddellijke rapportage aan ►M2 het directoraat Veiligheid van de Commissie ◄ of de nationale veiligheidsinstantie van de lidstaat die het initiatief heeft genomen tot het toezenden van de documenten (met een kopie van het verslag aan ►M2 het directoraat Veiligheid van de Commissie ◄);

b) uitvoering van een onderzoek en na afloop daarvan volledige rapportage aan de onder a) bedoelde instanties. Vervolgens worden de vereiste maatregelen vastgesteld om het probleem op te lossen.

17. Inspecties

►M2 Het directoraat Veiligheid van de Commissie ◄ wordt door middel van een overeenkomst met de betrokken staten of internationale organisaties gemachtigd een evaluatie uit te voeren van de doeltreffendheid van de maatregelen ter bescherming van de vrijgegeven gerubriceerde EU-gegevens.

18. Rapportage

Onder voorbehoud van de sluiting van een beveiligingsovereenkomst brengt de staat of internationale organisatie die de gerubriceerde EU-gegevens onder zich houdt jaarlijks, op een bij de instemming met de vrijgave van de gegevens gespecificeerde datum, verslag uit om te bevestigen dat deze veiligheidsvoorschriften zijn nageleefd.

▼B

Aanhangsel 5

Richtsnoeren voor de vrijgave van gerubriceerde EU-gegevens aan derde staten of internationale organisaties: derdegraadssamenwerking

PROCEDURES

1. In bepaalde gevallen kan de Commissie het wenselijk achten om onder bepaalde speciale omstandigheden samen te werken met staten of organisaties die niet de door deze veiligheidsvoorschriften vereiste garanties kunnen bieden terwijl de gewenste samenwerking wel noopt tot vrijgave van gerubriceerde EU-gegevens.

2. De bevoegdheid om gerubriceerde EU-gegevens vrij te geven aan derde staten of internationale organisaties, waarvan het beleid en de voorschriften inzake beveiliging aanzienlijk verschillen van die van de EU, berust bij de opsteller. De bevoegdheid om binnen de Commissie gecreëerde EUCI vrij te geven berust bij de Commissie als college.

   In beginsel is de bevoegdheid beperkt tot gegevens met een rubricering tot en met ►M1 SECRET UE ◄; gerubriceerde gegevens die beschermd worden door bijzondere beveiligingsindicatoren of markeringen zijn hiervan uitgesloten.

3. De Commissie beoordeelt de opportuniteit van de vrijgave van gerubriceerde gegevens en de noodzaak van de begunstigden om kennis te nemen van de gegevens, en besluit vervolgens over de aard van de gerubriceerde gegevens die kunnen worden meegedeeld.

4. Indien de Commissie voorstander is van vrijgave, zal het voor veiligheid bevoegde Commissielid

   — het advies inwinnen van de opstellers van de vrij te geven EUCI;

   — een bijeenkomst beleggen van de Adviesgroep Veiligheidsbeleid van de Commissie of zo nodig, volgens een stilzwijgende procedure, navraag doen bij de nationale veiligheidsinstanties van de lidstaten om het technisch advies van de Adviesgroep Veiligheidsbeleid van de Commissie in te winnen.

5. Het advies van de Adviesgroep Veiligheidsbeleid van de Commissie behelst:

   a) een evaluatie van de veiligheidsrisico's waaraan de EU of haar lidstaten blootstaan;

   b) de rubriceringsgraad van de gegevens die mogen worden vrijgegeven;

   c) lagere rubricering of derubricering voordat de gegevens worden vrijgegeven;

   d) procedures voor de verwerking van de vrij te geven documenten (zie punt hieronder);

   e) de mogelijke methoden voor de overdracht (gebruik van openbare postdiensten, openbare of beveiligde telecommunicatiesystemen, diplomatieke koerier, gemachtigde koeriers, enz.).

6. De documenten die worden vrijgegeven aan de in dit aanhangsel bedoelde staten of organisaties worden in beginsel verstrekt zonder referentie naar de bron of EU-rubricering. De Adviesgroep Veiligheidsbeleid van de Commissie kan de volgende aanbevelingen doen:

   — het gebruik van een specifieke markering of code;

   — het gebruik van een specifiek rubriceringssysteem waarbij de controlemaatregelen met betrekking tot de methoden die de begunstigde gebruikt voor de overdracht van documenten worden afgestemd op de gevoeligheid van de gegevens.

▼B

7. ►M2 Het voor veiligheid bevoegde Commissielid ◄ stuurt het advies van de Adviesgroep Veiligheidsbeleid van de Commissie door naar de Commissie, die daarover een besluit neemt.

8. Zodra de Commissie heeft ingestemd met de vrijgave van gerubriceerde EU-gegevens en met de praktische uitvoeringsprocedures legt ►M2 het directoraat Veiligheid van de Commissie ◄ de nodige contacten met de beveiligingsinstanties van de betrokken staat of organisatie om de toepassing van de beoogde beveiligingsmaatregelen te vergemakkelijken.

9. Het voor veiligheid bevoegde Commissielid informeert de lidstaat over de aard en de rubricering van de gegevens, en geeft daarbij een lijst van organisaties en landen waarvoor de gegevens mogen worden vrijgegeven zoals door de Commissie is besloten.

10. ►M2 Het directoraat Veiligheid van de Commissie ◄ neemt de nodige maatregelen om latere schade-evaluaties en herzieningen van de procedures te vergemakkelijken

Mochten de voorwaarden voor samenwerking veranderen, dan zal de Commissie de zaak opnieuw bekijken.

VEILIGHEIDSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

11. Het voor veiligheid bevoegde Commissielid deelt het besluit van de Commissie om vrijgave van gerubriceerde EU-gegevens toe te staan, mee aan de begunstigde staten of internationale organisaties, samen met de nadere bepalingen inzake bescherming die door de Adviesgroep Veiligheidsbeleid van de Commissie zijn voorgesteld en door de Commissie zijn goedgekeurd.

12. Het besluit houdende vrijgave treedt niet eerder in werking dan nadat de begunstigden schriftelijk hebben verzekerd dat zij:

— de gegevens niet voor andere doeleinden zullen gebruiken dan voor de door de Commissie goedgekeurde samenwerking;

— de gegevens op de door de Commissie vereiste wijze zullen beschermen.

13. Overdracht van documenten

a) De praktische procedures voor de overdracht van documenten worden geregeld tussen ►M2 het directoraat Veiligheid van de Commissie ◄ en de veiligheidsinstanties van de ontvangende staten of internationale organisaties. Hierbij zullen in het bijzonder de exacte adressen worden gespecificeerd waarnaar de documenten moeten worden gestuurd.

b) Als ►M1 CONFIDENTIEL UE ◄ en hoger gerubriceerde documenten worden in een dubbele enveloppe doorgegeven. Op de binnenenveloppe wordt een specifiek stempel of specifieke code aangebracht en een vermelding van de speciale rubricering die voor het document is afgesproken. Voor elk gerubriceerd document wordt een ontvangstformulier ingesloten. Op het ontvangstformulier, dat zelf niet gerubriceerd is, worden enkel de bijzonderheden van het document (referentie, datum, kopienummer) en de taal waarin het is gesteld, maar niet de titel, vermeld.

c) De binnenenveloppe wordt in een buitenenveloppe verpakt, die voor ontvangstdoeleinden een paknummer krijgt. Op de buitenenveloppe wordt geen beveiligingsrubricering aangebracht.

d) Koeriers ontvangen altijd een ontvangstbewijs met het paknummer.

▼B

14. Registratie bij ontvangst

De nationale veiligheidsinstantie van de geadresseerde staat of haar tegenhanger in de staat die namens de regering de door de Commissie toegezonden gerubriceerde gegevens ontvangt of het beveiligingsbureau van de ontvangende internationale organisatie, legt een speciaal bestand aan om bij ontvangst gerubriceerde EU-gegevens te registreren. Dit bestand omvat kolommen voor de datum van ontvangst, de bijzonderheden van het document (datum, referentie- en kopienummer), de rubricering, de titel, de naam of de titel van de geadresseerde, de datum waarop het ontvangstbewijs is teruggestuurd en de datum waarop het document is teruggestuurd naar de EU of vernietigd is.

15. Gebruik en bescherming van de uitgewisselde gerubriceerde gegevens

a) Als ►M1 SECRET UE ◄ gerubriceerde gegevens worden verwerkt door speciaal daarvoor aangewezen functionarissen die gemachtigd zijn om toegang te hebben tot gegevens met een dergelijke rubricering. De gegevens worden opgeborgen in beveiligingsruimtes van goede kwaliteit die alleen geopend kunnen worden door personen die gemachtigd zijn om toegang te hebben tot de daarin bewaarde gegevens. De zones waarin deze ruimtes zich bevinden staan onder permanente bewaking en er wordt een verificatiesysteem opgezet om te garanderen dat deze zones alleen worden betreden door naar behoren gemachtigde personen. Als ►M1 SECRET UE ◄ gerubriceerde gegevens worden verzonden per diplomatieke koerier, beveiligde postdiensten en beveiligde telecommunicatiekanalen. Een ►M1 SECRET UE ◄-document mag alleen worden gekopieerd na schriftelijke toestemming van de autoriteit waarvan het afkomstig is. Alle kopieën worden geregistreerd en gevolgd. Voor alle handelingen in verband met ►M1 SECRET UE ◄-documenten worden ontvangstbewijzen uitgeschreven.

b) Als ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens worden verwerkt door speciaal daarvoor aangewezen functionarissen die gemachtigd zijn om over het onderwerp in kwestie geïnformeerd te worden. De documenten worden opgeslagen in afgesloten beveiligingsruimtes in gecontroleerde zones.

Als ►M1 CONFIDENTIEL UE ◄ gerubriceerde gegevens worden verstuurd per diplomatieke koerier, militaire postdiensten en beveiligde telecommunicatiekanalen. Kopieën mogen worden gemaakt door de ontvangende instantie, waarbij het aantal en de distributie worden geregistreerd in speciale bestanden.

c) Als ►M1 RESTREINT UE ◄ gerubriceerde gegevens worden verwerkt in locaties die niet toegankelijk zijn voor niet-gemachtigd personeel en worden opgeslagen in afgesloten opbergmiddelen. Documenten mogen per openbare postdiensten worden verstuurd als aangetekende zending in een dubbele enveloppe en, in noodsituaties tijdens operaties, via onbeschermde openbare telecommunicatiesystemen. De ontvangers maken kopieën van de documenten.

d) Niet-gerubriceerde gegevens vereisen geen speciale beschermingsmaatregelen en mogen worden verstuurd per post en openbare telecommunicatiesystemen. De geadresseerden mogen kopieën van de gegevens maken.

16. Vernietiging

Overtollige documenten worden vernietigd. In geval van als ►M1 RESTREINT UE ◄ en ►M1 CONFIDENTIEL UE ◄ gerubriceerde documenten wordt van de vernietiging aantekening gemaakt in de speciale bestanden. In geval van als ►M1 SECRET UE ◄ gerubriceerde documenten wordt een proces-verbaal van vernietiging opgesteld en ondertekend door twee getuigen van de vernietiging.

17. Inbreuken op de veiligheidsvoorschriften

Wanneer als ►M1 CONFIDENTIEL UE ◄ of ►M1 SECRET UE ◄ gerubriceerde gegevens zijn gecompromitteerd of vermoedelijk zijn gecompromitteerd voert de nationale veiligheidsinstantie van de staat of het hoofd van de veiligheidsdienst van de organisatie een onderzoek uit naar de omstandigheden van de compromittering. De resultaten worden meegedeeld aan ►M2 het directoraat Veiligheid van de Commissie ◄. Indien het ontoereikende procedures of opslagmethodes zijn die tot de compromittering hebben geleid, worden de nodige stappen gezet om deze te verbeteren.

▼B

Aanhangsel 6

LIJST VAN AFKORTINGEN

ACPC	Raadgevende commissie voor aankopen en overeenkomsten (Advisory Committee on Procurement and Contracts)
CrA	Crypto-autoriteit (Crypto Authority)
CISO	Centrale informatiebeveiligingsfunctionaris (Central Informatics Security Officer)
COMPUSEC	Computerbeveiliging (Computer Security)
COMSEC	Communicatiebeveiliging (Communication Security)
CSO	►M2 het directoraat Veiligheid van de Commissie ◄ (Commission Security Office)
ESDP	Europees veiligheids- en defensiebeleid (European Security and Defense Policy)
EUCI	Gerubriceerde EU-gegevens (EU classified information)
IA	INFOSEC-autoriteit (INFOSEC Authority)
INFOSEC	Informatiebeveiliging (Information Security)
IO	Informatie-eigenaar (Information Owner)
ISO	Internationale Organisatie voor normalisatie (International Organisation for Standardisation)
IT	Informatietechnologie (Information Technology)
LISO	Plaatselijke informatiebeveiligingsfuntionaris (Local Informatics Security Officer)
LSO	Plaatselijke veiligheidsfunctionaris (Local Security Officer)
MSO	Beveiligingsfunctionaris voor de vergadering (Meeting Security Officer)
NSA	Nationale veiligheidsinstantie (National Security Authority)
PC	Personal Computer
RCO	Functionaris voor de registercontrole (Registry Control Officer)
SAA	Autoriteit voor veiligheidsaccreditatie (Security Accreditation Authority)
SecOPS	Operationele beveiligingsprocedures (Security Operating Procedures)
SSRS	Systeemgebonden specificatie van beveiligingseisen (Specific Security Requirement Statement)
TA	Tempest-autoriteit (Tempest Authority)
TSO	Eigenaar technisch systeem (Technical Systems Owner)

▼M3

DSA	Aangewezen veiligheidsinstantie (Designated Security Authority)
FSC	Veiligheidsmachtiging voor een vestiging (Facility Security Clearance)
FSO	Veiligheidsfunctionaris voor een vestiging (Facility Security Officer)
PSC	Veiligheidsmachtiging voor het personeel (Personnel Security Clearance)
SAL	Memorandum over de beveiligingsaspecten (Security Aspects Letter)
SCG	Gids voor beveiligingsrubricering (Security Classification Guide)