II

(Besluiten waarvan de publicatie niet voorwaarde is voor de toepassing)

RAAD

BESLUIT VAN DE RAAD

van 19 maart 2001

tot vaststelling van beveiligingsvoorschriften van de Raad

(2001/264/EG)

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, inzonderheid op artikel 207, lid 3,

Gelet op Besluit 2000/396/EG, EGKS, Ewaton van de Raad van 5 juni 2000 houdende vaststelling van zijn reglement van orde [1], inzonderheid op artikel 24,

Overwegende hetgeen volgt:

(1) Teneinde de Raadswerkzaamheden op gebieden die tot een zekere mate van vertrouwelijkheid nopen tot ontwikkeling te brengen, is het dienstig een integraal beveiligingssysteem op te zetten dat de Raad, het secretariaat-generaal daarvan en de lidstaten omvat.

(2) In een dergelijk systeem moet de inhoud van alle voorgaande besluiten en bepalingen op dit gebied in één tekst bijeengebracht worden.

(3) In de praktijk zal het grootste gedeelte van de als „CONFIDENTIEL UE" of hoger gerubriceerde EU-gegevens betrekking hebben op het gemeenschappelijk veiligheids- en defensiebeleid.

(4) Teneinde de doeltreffendheid van het aldus opgezette beveiligingssysteem te waarborgen, dienen de lidstaten bij het functioneren te worden betrokken doordat zij de nationale maatregelen treffen die noodzakelijk zijn om, wanneer hun bevoegde autoriteiten en ambtenaren gerubriceerde EU-gegevens verwerken, te voldoen aan de bepalingen van dit besluit.

(5) De Raad verwelkomt het voornemen van de Commissie om op de datum van toepassing van dit besluit een integraal systeem in te voeren dat strookt met de bijlage bij dit besluit, teneinde te zorgen voor een soepele besluitvorming van de Unie.

(6) De Raad onderstreept het belang, waar dienstig, het Europees Parlement en de Commissie te betrekken bij de voorschriften en normen voor vertrouwelijkheid die noodzakelijk zijn ter bescherming van de belangen van de Unie en haar lidstaten.

(7) Dit besluit laat artikel 255 van het Verdrag en de instrumenten ter uitvoering daarvan onverlet.

(8) Dit besluit laat bestaande praktijken van de lidstaten met betrekking tot de informatie van hun nationale parlementen over de werkzaamheden van de Unie onverlet,

BESLUIT:

Artikel 1

De beveiligingsvoorschriften van de Raad in de bijlage worden hierbij goedgekeurd.

Artikel 2

1. De secretaris-generaal/hoge vertegenwoordiger neemt passende maatregelen om te zorgen dat wanneer gerubriceerde EU-gegevens worden verwerkt, de in artikel 1 bedoelde voorschriften in het secretariaat-generaal van de Raad (hierna „SGR" te noemen) door de SGR-ambtenaren en andere personeelsleden, door de contractanten van het SGR en door het bij het SGR gedetacheerd personeel, zowel op de locaties van de Raad als in de gedecentraliseerde EU-organen worden nageleefd [2].

[1] PB L 149 van 23.6.2000, blz. 21.

[2] Zie conclusies van de Raad van 10.11.2000.

2. De lidstaten nemen, in overeenstemming met hun nationale regelingen, passende maatregelen om te zorgen dat wanneer gerubriceerde EU-gegevens worden verwerkt, de in artikel 1 bedoelde voorschriften worden nageleefd door hun diensten en op hun locaties 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 Raad of van de instanties ervan bijwonen, of deelnemen aan andere Raadswerkzaamheden,

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 van de lidstaten en het gedetacheerd personeel, die gerubriceerde EU-gegevens verwerken.

De lidstaten stellen het SGR onverwijld in kennis van de genomen maatregelen.

3. De in de leden 1 en 2 bedoelde maatregelen worden voor 30 november 2001 genomen.

Artikel 3

Overeenkomstig de grondbeginselen en minimumbeveiligingsnormen als bedoeld in deel I van de bijlage kan de secretaris-generaal/hoge vertegenwoordiger maatregelen nemen overeenkomstig deel II, afdeling I, punt 1 en punt 2, van de bijlage.

Artikel 4

Het onderhavige besluit vervangt vanaf de dag van zijn toepassing:

a) Besluit 98/319/EG van de Raad van 27 april 1998 betreffende de regeling inzake de machtiging van ambtenaren en personeelsleden van het secretariaat-generaal van de Raad voor de raadpleging van gerubriceerde gegevens die de Raad in zijn bezit heeft [1];

b) besluit van de secretaris-generaal van de Raad/hoge vertegenwoordiger van 27 juli 2000 inzake maatregelen betreffende de bescherming van gerubriceerde gegevens die op het secretariaat-generaal van de Raad van toepassing zijn [2];

c) Besluit nr. 433/97 van 22 mei 1997 van de secretaris-generaal van de Raad betreffende de procedure tot screening van de ambtenaren die belast zijn met de werking van het Cortesy-systeem.

Artikel 5

1. Dit besluit wordt van kracht op de dag van zijn bekendmaking.

2. Het is van toepassing vanaf 1 december 2001.

Gedaan te Brussel, 19 maart 2001.

Voor de Raad

De voorzitter

A. LINDH

[1] PB L 140 van 12.5.1998, blz. 12.

[2] PB C 239 van 23.8.2000, blz. 1.

BIJLAGE

BEVEILIGINGSVOORSCHRIFTEN VAN DE RAAD VAN DE EUROPESE UNIE

INHOUD

Bladzijde

Bladzijde

Aanhangsels

DEEL I

GRONDBEGINSELEN EN MINIMUMNORMEN VOOR DE BEVEILIGING

INLEIDING

1. Bij deze bepalingen worden de grondbeginselen en minimumnormen voor de beveiliging vastgesteld die door de Raad, het secretariaat-generaal van de Raad (hierna te noemen „SGR"), de lidstaten en de gedecentraliseerde organen van de Europese Unie (hierna te noemen „gedecentraliseerde EU-organen") op passende wijze moeten worden nageleefd, zodat de beveiliging is gewaarborgd en ieder ervan verzekerd is dat er een gemeenschappelijke norm van bescherming is ingesteld.

2. Onder gerubriceerde EU-gegevens wordt verstaan: gegevens en materiaal waarvan openbaarmaking zonder machtiging de belangen van de EU of van een of meer van haar lidstaten, naargelang het geval in meerdere of mindere mate zou kunnen schaden, ongeacht of dergelijke gegevens afkomstig zijn van de EU, de lidstaten, derde staten of internationale organisaties.

3. In deze voorschriften wordt verstaan onder

   a) 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 fysiek medium waarop gegevens zijn opgeslagen;

   b) materiaal: een document als bedoeld onder a), alsook enig onderdeel van uitrusting of wapens dat gefabriceerd is of wordt.

4. Met de beveiliging worden de volgende hoofddoelstellingen beoogd:

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

   b) bescherming van EU-gegevens die in communicatie- en informatiesystemen en -netwerken worden verwerkt tegen gevaren voor de integriteit en de beschikbaarheid ervan;

   c) beveiliging van installaties die EU-gegevens bevatten tegen sabotage en kwaadwillige beschadiging;

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

5. De fundamenten voor een goede beveiliging zijn:

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

      i) het vergaren en vastleggen van inlichtingen over spionage, sabotage, terrorisme en andere subversieve activiteiten; en

      ii) het informeren en adviseren van haar regering en via deze de Raad, over de aard van de bedreigingen voor de veiligheid en de middelen om zich daartegen te beschermen;

   b) de aanwezigheid in iedere lidstaat en in het SGR van een technische gegevensbeveiligingsinstantie (INFOSEC), die met de betrokken Veiligheidsinstantie meewerkt aan het verschaffen van informatie en advies over technische bedreigingen voor de veiligheid en de middelen om zich daartegen te beschermen;

   c) regelmatige samenwerking tussen de regeringsdepartementen, -organen en relevante diensten van het SGR, met het oog op besluiten, respectievelijk aanbevelingen inzake:

      i) de gegevens, middelen en installaties die beschermd moeten worden; en

      ii) gemeenschappelijke normen voor de bescherming.

6. Wat de vertrouwelijkheid betreft, zijn aandacht en ervaring vereist bij de selectie van te beschermen gegevens en materiaal en de beoordeling van de mate van bescherming die noodzakelijk is. Het is van fundamenteel belang dat de mate van bescherming correspondeert met de veiligheidsgevoeligheid van bepaalde gegevens of bepaald materiaal. Om te zorgen dat de informatiestroom soepel verloopt, moeten stappen worden genomen ter voorkoming over rubricering. Het rubriceringssysteem is het instrument waarmee gevolg wordt gegeven aan deze beginselen; een soortgelijk rubriceringssysteem moet gebruikt worden voor het plannen en organiseren van de bestrijding van spionage, sabotage, terrorisme en andere bedreigingen, zodat de grootste mate van bescherming gegeven wordt aan de belangrijkste locaties die gerubriceerde gegevens bevatten en binnen die locatie aan de gevoeligste elementen.

GRONDBEGINSELEN

7. **De beveiligingsmaatregelen dienen:**

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

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

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

d) er voor te zorgen dat gerubriceerde gegevens alleen verspreid worden op basis van het „need-to-know"-beginsel (noodzaak van kennisneming) dat fundamenteel is voor alle beveiligingsaspecten;

e) waarborgen te 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 die 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.

ORGANISATIE VAN DE BEVEILIGING

Gemeenschappelijke minimumnormen

8. De Raad en alle lidstaten dienen ervoor te zorgen dat in alle administratieve onderdelen en/of regeringsdepartementen, andere EU-instellingen en -organen en bij contractanten van de EU, gemeenschappelijke minimumnormen voor de beveiliging in acht worden genomen, 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.

PERSONEELSGERELATEERDE BEVEILIGING

Veiligheidsonderzoek van het personeel

9. Alle personen die toegang moeten hebben tot als 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 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) een zodanig karakter en een zodanige discretie bezitten dat hun betrouwbaarheid op het stuk van het verwerken van gerubriceerde gegevens buiten kijf staat; of

c) kwetsbaar zijn voor druk van externe of andere bronnen, bijvoorbeeld in verband met een eerdere verblijfplaats of vroegere betrekkingen die een gevaar zouden kunnen opleveren voor de veiligheid.

Bij het onderzoek dient bijzondere aandacht te worden geschonken aan de personen die:

d) toegang zullen krijgen tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens;

e) functies bekleden die regelmatige toegang tot een aanzienlijke hoeveelheid als SECRET UE gerubriceerde gegevens met zich meebrengen;

f) door hun functie speciale toegang hebben tot voor een taak beslissende communicatie- of informatiesystemen en die derhalve in de gelegenheid zijn zonder machtiging toegang te krijgen tot grote hoeveelheden gerubriceerde EU-gegevens of de taak ernstig te schaden door technische sabotage.

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

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

Machtigingsgegevens van het personeel

11. Alle diensten, organen of vestigingen die gerubriceerde EU-gegevens verwerken of voor de taak beslissende communicatie- of informatiesystemen huisvesten houden de machtigingsgegevens van het personeel dat daarvoor benoemd is bij. Elke machtiging wordt geverifieerd wanneer de gelegenheid vereist dat deze passend is voor de vigerende taakomschrijving van die persoon; de machtiging wordt bij voorrang opnieuw onderzocht wanneer nieuwe informatie wordt ontvangen die erop wijst dat continuering van de taak bij gerubriceerde werkzaamheden niet langer strookt met de veiligheidsbelangen. De machtigingsgegevens worden beheerd door het hoofd van de beveiliging van de dienst, het orgaan of de vestiging.

Beveiligingsinstructies voor het personeel

12. Alle personeelsleden die werkzaam zijn in omstandigheden waarin zij toegang zouden kunnen krijgen tot gerubriceerde gegevens, dienen bij het opnemen van hun taak en vervolgens met regelmatige tussenpozen grondige instructies te krijgen over de noodzaak van beveiliging en de procedures om die beveiliging door te voeren. Als procedure is het nuttig om te eisen dat al deze personeelsleden schriftelijk bevestigen dat zij de beveiligingsvoorschriften die voor hun taak relevant zijn volledig begrijpen.

Beheersverantwoordelijkheden

13. Leidinggevenden zijn verplicht de leden van hun personeel die betrokken zijn bij gerubriceerde werkzaamheden of toegang hebben tot voor de taak beslissende communicatie- of informatiesystemen te kennen en moeten incidenten of duidelijk zwakke plekken, die op de veiligheid van invloed zouden kunnen zijn, vastleggen en rapporteren.

Veiligheidsstatus van het personeel

14. Er worden procedures ingesteld om ervoor te zorgen dat, wanneer over een persoon negatieve informatie bekend wordt, bepaald wordt of deze betrokken is bij gerubriceerde werkzaamheden of toegang heeft tot voor de taak beslissende communicatie- of informatiesystemen; indien wordt geconstateerd dat genoemde persoon een veiligheidsrisico met zich meebrengt, wordt de betrokken instantie op de hoogte gebracht en wordt de persoon uitgesloten of verwijderd van taken waar hij de veiligheid in gevaar zou kunnen brengen.

FYSIEKE BEVEILIGING

De noodzaak van bescherming

15. De fysieke beveiligingsmaatregelen die worden toegepast om de bescherming van gerubriceerde EU-gegevens te waarborgen dienen evenredig te zijn aan de rubriceringsgraad, de omvang en de bedreiging van de aanwezige gegevens en materiaal. Daarom moet zowel over- als onderrubricering vermeden worden en moet de rubricering regelmatig herzien worden. Alle houders van gerubriceerde EU-gegevens dienen voor de rubricering van die gegevens uniforme praktijken te volgen en moeten voldoen aan gemeenschappelijke normen voor de bescherming wat betreft bewaring, overdracht en verwijdering van te beschermen gegevens en materiaal.

Controle

16. Alvorens zones die gerubriceerde EU-gegevens bevatten onbemand achter te laten, dienen de personen die met de bewaring zijn belast ervoor te 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.

Beveiliging van gebouwen

17. Gebouwen waarin gerubriceerde EU-gegevens of voor de taak beslissende communicatie- en informatiesystemen zijn gehuisvest, dienen beschermd te worden tegen ongeoorloofde toegang. 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.

18. 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 indien 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.

Calamiteitenplannen

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

BEVEILIGING VAN INFORMATIE (INFOSEC)

20. „INFOSEC" heeft betrekking op de keuze en de toepassing van beveiligingsmaatregelen ter bescherming van gegevens die worden verwerkt, opgeslagen of overgedragen in communicatie-, informatie- en andere elektronische systemen tegen accidenteel of intentioneel veroorzaakt verlies van vertrouwelijkheid, integriteit of beschikbaarheid. Er dienen passende tegenmaatregelen te worden genomen om te voorkomen dat niet-gemachtigde gebruikers toegang krijgen tot EU-gegevens, dat gemachtigde gebruikers de toegang tot EU-gegevens onmogelijk wordt gemaakt en om te zorgen dat corruptie, ongeoorloofde wijziging of verwijdering van EU-gegevens wordt voorkomen.

BEVEILIGING TEGEN SABOTAGE EN ANDERE VORMEN VAN KWAADWILLIGE BESCHADIGING

21. Fysieke voorzorgen ter bescherming van belangrijke installaties waarin zich gerubriceerde gegevens bevinden bieden als beveiligingsmaatregelen de beste bescherming tegen sabotage en kwaadwillige beschadiging; het veiligheidsonderzoek van het personeel alleen is daarvoor geen effectief vervangmiddel. De bevoegde nationale instantie dient inlichtingen te vergaren over spionage, sabotage, terrorisme en andere subversieve activiteiten.

VRIJGAVE VAN GERUBRICEERDE GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES

22. Het besluit om van de Raad afkomstige gerubriceerde EU-gegevens vrij te geven aan een derde staat of een internationale organisatie wordt door de Raad genomen. Indien de gegevens waarvan de vrijgave gewenst wordt niet afkomstig zijn van de Raad, vraagt de Raad vóór vrijgave toestemming aan de bron. Indien de bron niet kan worden vastgesteld, neemt de Raad de verantwoordelijkheid over.

23. Wanneer de Raad van derde staten of 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 beveiligingsvoorschriften worden vastgesteld voor gerubriceerde EU-gegevens, of strengere normen als geëist door de derde die de gegevens vrijgeeft. Er kan een regeling worden getroffen voor wederzijdse controle.

24. Bovenstaande beginselen worden geïmplementeerd overeenkomstig de nadere bepalingen van deel II.

DEEL II

AFDELING I

DE ORGANISATIE VAN DE BEVEILIGING BINNEN DE RAAD VAN DE EUROPESE UNIE

De secretaris-generaal/hoge vertegenwoordiger

1. De secretaris-generaal/hoge vertegenwoordiger:

   a) voert het beveiligingsbeleid van de Raad uit;

   b) bestudeert de door de Raad of de bevoegde organen daarvan voorgelegde beveiligingsproblemen;

   c) onderzoekt in nauwe samenwerking met de nationale veiligheidsinstanties (of andere relevante instanties) van de lidstaten (hierna NVI genoemd) de vraagstukken die veranderingen in het beveiligingsbeleid van de Raad met zich meebrengen. In aanhangsel 1 staat een lijst van deze autoriteiten.

2. De secretaris-generaal/hoge vertegenwoordiger is meer bepaald verantwoordelijk voor:

   a) de coördinatie van alle beveiligingsaangelegenheden die verband houden met de werkzaamheden van de Raad;

   b) het richten van een verzoek tot elke lidstaat om een centraal TRÈS SECRET UE/EU TOP SECRET-register op te zetten en te eisen dat in de gedecentraliseerde EU-organen, waar passend, eveneens een dergelijk register wordt opgezet;

   c) het richten van verzoeken tot de daartoe aangewezen instanties van de lidstaten om de NVI beveiligingsmachtigingen te verstrekken voor personeel in dienst van het SGR overeenkomstig afdeling VI;

   d) het onderzoeken of doen onderzoeken van lekken van gerubriceerde EU-gegevens die zich, tot bewijs van het tegendeel, hebben voorgedaan in het SGR of in een van de gedecentraliseerde EU-organen;

   e) het richten van een verzoek tot de relevante veiligheidsinstanties om een onderzoek in te leiden, wanneer er buiten het SGR of de gedecentraliseerde EU-organen, gerubriceerde EU-gegevens uitgelekt zijn en voor de coördinatie van de onderzoeken wanneer er meerdere veiligheidsinstanties bij zijn betrokken;

   f) het gezamenlijk en met overeenstemming van de betrokken NVI uitvoeren van periodieke onderzoeken van de beveiligingsregelingen voor de bescherming van gerubriceerde EU-gegevens in de lidstaten;

   g) het onderhouden van nauwe contacten met alle betrokken veiligheidsinstanties, teneinde te komen tot een algehele coördinatie van de beveiliging;

   h) het beleid en de procedures van de Raad inzake beveiliging voortdurend in het oog houden en zo nodig passende aanbevelingen doen. Daartoe legt hij het door de Dienst beveiliging van het SGR opgestelde jaarlijkse inspectieplan aan de Raad voor.

Het Beveiligingscomité van de Raad

3. Er wordt een Beveiligingscomité opgericht, bestaand uit vertegenwoordigers van de NVI's van de lidstaten. Het comité wordt voorgezeten door de secretaris-generaal/hoge vertegenwoordiger of zijn vertegenwoordiger. Er kunnen ook vertegenwoordigers van de gedecentraliseerde EU-organen worden uitgenodigd wanneer er aangelegenheden worden besproken die hen aanbelangen.

4. Het Beveiligingscomité komt volgens instructies van de Raad bijeen op verzoek van de secretaris-generaal/hoge vertegenwoordiger of een NVI. Het comité heeft de bevoegdheid alle beveiligingsaangelegenheden in verband met de werkzaamheden van de Raad te onderzoeken en te evalueren en zo nodig aanbevelingen tot de Raad te richten. Het comité heeft tevens de bevoegdheid met betrekking tot de werkzaamheden van het SGR aanbevelingen over beveiligingsaangelegenheden te richten tot de secretaris-generaal/hoge vertegenwoordiger.

De Dienst beveiliging van het secretariaat-generaal van de Raad

5. Voor de uitoefening van zijn verantwoordelijkheden als bedoeld in de punten 1 en 2 beschikt de secretaris-generaal/hoge vertegenwoordiger over de Dienst beveiliging van het SGR voor het coördineren van, toezicht houden op en implementeren van de beveiligingsmaatregelen.

6. Het hoofd van de Dienst beveiliging van het SGR is de belangrijkste adviseur van de secretaris-generaal/hoge vertegenwoordiger inzake beveiligingsaangelegenheden; hij treedt op als secretaris van het Beveiligingscomité. In dit verband leidt hij de actualisering van de beveiligingsvoorschriften en coördineert hij de beveiligingsmaatregelen met de bevoegde instanties van de lidstaten en, waar van toepassing, de internationale organisaties waarmee de Raad beveiligingsovereenkomsten heeft gesloten. Met het oog daarop treedt hij op als verbindingsambtenaar.

7. Het hoofd van de Dienst beveiliging van het SGR is verantwoordelijk voor de accreditatie van IT-systemen en -netwerken binnen het SGR. Het hoofd van de Dienst beveiliging van het SGR en de betrokken NVI besluiten waar nodig gezamenlijk over de accreditatie van IT-systemen en -netwerken waarbij het SGR, de lidstaten, de gedecentraliseerde EU-organen en/of derde partijen (staten of internationale organisaties) zijn betrokken.

Gedecentraliseerde EU-organen

8. Elke directeur van een gedecentraliseerd EU-orgaan is verantwoordelijk voor de implementatie van de beveiliging in zijn instelling. Normaliter benoemt hij een personeelslid dat terzake tegenover hem verantwoordelijk is. Dit personeelslid wordt benoemd als beveiligingsfunctionaris.

Lidstaten

9. Iedere lidstaat wijst een NVI aan die verantwoordelijk is voor de beveiliging van gerubriceerde EU-gegevens ([1]).

10. In het kader van de overheidsdiensten van elke lidstaat is de corresponderende NVI verantwoordelijk voor

    a) de beveiliging van de gerubriceerde EU-gegevens die in het bezit zijn van publieke of particuliere, in binnen- of buitenland gevestigde nationale departementen, lichamen of organen;

    b) de machtiging voor de instelling van TRÈS SECRET UE/EU TOP SECRET-registers (deze bevoegdheid kan worden gedelegeerd aan de TRÈS SECRET UE/EU TOP SECRET-controlefunctionaris van een Centraal register);

    c) de periodieke inspectie van beveiligingsregelingen voor de bescherming van gerubriceerde EU-gegevens;

    d) de zorg dat alle eigen onderdanen en buitenlanders die werkzaam zijn bij een nationaal departement, lichaam of orgaan, die toegang kunnen krijgen tot als TRÈS SECRET UE/ EU TOP SECRET, SECRET UE en CONFIDENTIEL EU gerubriceerde EU-gegevens een veiligheidsmachtiging hebben;

    e) het opstellen van beveiligingsplannen die noodzakelijk geacht worden om te voorkomen dat gerubriceerde EU-gegevens in de handen van niet-gemachtigden vallen.

Wederzijdse veiligheidsinspecties

11. De Dienst beveiliging van het SGR en de betrokken NVI verrichten gezamenlijk en met wederzijdse instemming ([2]) periodieke inspecties van de beveiligingsregelingen ter bescherming van de gerubriceerde EU-gegevens in het SGR en in de permanente vertegenwoordigingen van de lidstaten bij de Europese Unie, alsmede in de lokalen van de lidstaten in de gebouwen van de Raad.

12. De Dienst beveiliging van het SGR of, op verzoek van de secretaris-generaal, de NVI van de gastlidstaat, verrichten periodieke inspecties van de veiligheidsregelingen ter bescherming van gerubriceerde EU-gegevens in de gedecentraliseerde EU-organen.

([1]) Voor een lijst van de NVI die verantwoordelijk zijn voor de beveiliging van gerubriceerde EU-gegevens, zie aanhangsel 1.
([2]) Onverminderd het Verdrag van Wenen inzake diplomatiek verkeer van 1961.

AFDELING II

RUBRICERINGEN EN MARKERINGEN

RUBRICERINGSGRADEN ([1])

De volgende rubriceringsgraden worden gehanteerd:

1. TRÈS 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.

2. 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.

3. 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.

4. 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.

MARKERINGEN

5. Er kan een waarschuwingsmarkering worden gebruikt waarmee het domein waarop het document betrekking heeft of een speciale verspreiding op need-to-know-basis wordt aangegeven.

6. De markering ESDP/PESD 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.

7. Sommige documenten, meer bepaald die welke betrekking hebben op informatietechnologie (IT)-systemen kunnen een extra markering dragen die aanvullende beveiligingsmaatregelen meebrengen als omschreven in de relevante regelingen.

HET AANBRENGEN VAN RUBRICERING EN MARKERING

8. Rubricering en markering worden als volgt aangebracht:

   a) op RESTREINT UE-documenten, met mechanische/elektronische middelen,

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

   c) op SECRET UE- en TRÈS SECRET UE/EU TOP SECRET-documenten, met mechanische middelen en met de hand.

([1]) Een vergelijkend overzicht met de beveiligingsniveaus van EU, NAVO, WEU en de lidstaten staat in aanhangsel 2.

AFDELING III

RUBRICERINGSBEHEER

1. 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.

2. De verantwoordelijkheid voor het rubriceren van de gegevens en een eventuele lagere rubricering of derubricering [1] berust uitsluitend bij de bron.

   Ambtenaren en andere personeelsleden van het SGR rubriceren de gegevens op een lager niveau of derubriceren deze op instructie van of met toestemming van hun directeur-generaal.

3. De gedetailleerde procedures voor de behandeling van gerubriceerde documenten dienen zo te zijn opgezet dat gegarandeerd wordt dat de documenten op een bij de daarin vervatte gegevens passende wijze beschermd worden.

4. Het aantal personen dat gemachtigd is om TRÈS SECRET UE/EU TOP SECRET-documenten op te stellen wordt tot een minimum beperkt, hun namen worden op een lijst geplaatst en bijgehouden door het SGR, de lidstaten en waar van toepassing de gedecentraliseerde EU-organen.

RUBRICERING

5. De rubricering van een document wordt bepaald door het niveau van gevoeligheid van de inhoud overeenkomstig de definitie in afdeling II, punten 1 tot en met 4. Het is van belang dat er een correct en spaarzaam gebruik wordt gemaakt van rubricering. Dit geldt in het bijzonder voor de rubricering TRÈS SECRET UE/EU TOP SECRET.

6. De opsteller van een document dat gerubriceerd moet worden houdt rekening met de hierboven uiteengezette voorschriften en corrigeert neigingen tot over- of onderrubricering.

   Hoewel een hoge rubriceringsgraad voor een document op het eerste gezicht meer garanties lijkt te bieden kan routinematige overrubricering het vertrouwen in de geldigheid van het rubriceringssysteem schaden.

   Anderzijds moeten documenten niet te laag gerubriceerd worden met het oogmerk de beperkingen die bescherming met zich meebrengt, te omzeilen.

   Aanhangsel 3 bevat een praktische rubriceringsgids.

7. 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.

8. 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.

LAGERE RUBRICERING EN DERUBRICERING

9. 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 instelling, lidstaat, het bureau, de „opvolgerorganisatie" of de hogere autoriteit, waarvan het document afkomstig is, 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.

10. 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.

---

[1] Een lagere rubricering (downgrading) is een verlaging van het niveau van rubricering; derubricering (declassification) is de opheffing van een rubricering.

AFDELING IV

FYSIEKE BEVEILIGING

ALGEMEEN

1. De belangrijkste doelstelling van de fysieke beveiligingsmaatregelen is te verhinderen dat een niet-gemachtigde persoon toegang krijgt tot EU-gegevens en/of -materiaal die gerubriceerd zijn.

BEVEILIGINGSEISEN

2. Alle locaties, zones, gebouwen, bureaus, kamers, communicatie- en informatiesystemen, enz., waarin gerubriceerde EU-gegevens en gerubriceerd EU-materiaal bewaard en/of verwerkt worden, moeten beschermd worden door passende fysieke beveiligingsmaatregelen.

3. Om te bepalen welke mate van bescherming door fysieke beveiligingsmaatregelen noodzakelijk is, wordt er rekening gehouden met alle relevante factoren, zoals:

   a) de rubricering van de informatie 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, meer bepaald in de vorm van sabotage, terrorisme en andere subversieve en/of criminele activiteiten.

4. Met de fysieke beveiligingsmaatregelen wordt beoogd:

   a) het binnendringen door list of geweld te verhinderen;

   b) acties van malafide personeelsleden af te schrikken, tegen te houden en op te sporen (de spion in eigen gelederen);

   c) ambtenaren en andere personeelsleden van het SGR, van regeringsdepartementen van de lidstaten en/of andere instellingen of derde partijen die niet beantwoorden aan het „need-to-know"-criterium de toegang tot gerubriceerde EU-gegevens te ontzeggen.

FYSIEKE BEVEILIGINGSMAATREGELEN

Beveiligingszones

5. Zones waar als CONFIDENTIEL UE of hoger gerubriceerde gegevens worden verwerkt en opgeslagen worden zodanig opgezet en gestructureerd dat zij voldoen aan een van de volgende eisenpakketten:

   a) beveiligingszone van klasse I: een zone waar als 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 diegene die naar behoren en met goed gevolg zijn gescreend en speciaal gemachtigd zijn, de zone kunnen betreden;

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

   b) beveiligingszone van klasse II: een zone waar als CONFIDENTIEL UE of hoger gerubriceerde gegevens zodanig worden verwerkt en opgeslagen dat zij tegen toegang door niet gemachtigden kan worden beschermd door middel van intern opgezette controles, dat wil zeggen locaties met kantoren waar als 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 en met goed gevolg 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 van dienst aanwezig is, worden onmiddellijk na de normale werkuren geïnspecteerd, dit om te waarborgen dat gerubriceerde EU-gegevens veilig zijn weggeborgen.

Administratieve zone

6. Nabij of vóór de beveiligingszones van klasse I of klasse II kan een administratieve zone met een lager beveiligingsniveau 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 RESTREINT UE gerubriceerde gegevens worden verwerkt en opgeslagen.

Controles bij in- en uitgaan

7. Het betreden van beveiligingszones van klasse I en klasse II wordt gecontroleerd aan de hand van een pasje of een persoonsherkenningssysteem voor het vaste personeel. Ook wordt een systeem ingesteld om niet-gemachtigden de toegang tot gerubriceerde EU-gegevens te weigeren. 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.

Bewakingspatrouilles

8. Buiten de normale werkuren moet in de beveiligingszones 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 door de plaatselijke omstandigheden; een vuistregel is echter om de twee uur te patrouilleren.

Beveiligingsopbergmiddelen en braakwerende ruimten

9. Er worden drie klasses opbergmiddelen gebruikt voor de opslag van gerubriceerde EU-gegevens:

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

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

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

10. In braakwerende ruimten die zijn ingericht binnen een beveiligingszone van klasse I of klasse II, en voor alle beveiligingszones van klasse I waar als CONFIDENTIEL UE en hoger gerubriceerde gegevens zijn opgeslagen in rekken of is af te lezen van grafieken, kaarten, enz., dienen de muren, vloeren en plafonds, en de deur(en) met (een) slot(en) te worden gecertificeerd door een nationale veiligheidsinstantie (NVI) als zijnde van een gelijkwaardig beschermingsniveau als de klasse beveiligingsopbergmiddelen die zijn goedgekeurd voor de opslag van gegevens met dezelfde rubricering.

Sloten

11. Sloten op beveiligingsopbergmiddelen en braakwerende ruimten waarin gerubriceerde EU-gegevens worden opgeslagen, voldoen aan de volgende normen:

   — 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.

Controle van sleutels en codecombinaties

12. Sleutels van beveiligde opbergmiddelen mogen niet worden meegenomen buiten het gebouw. Codecombinaties van beveiligingsopbergmiddelen moeten worden gememoriseerd door personen die hiervan kennis moeten nemen. Bij gebruik in dringende gevallen is de beveiligingsambtenaar van het gebouw verantwoordelijk voor het bewaren van reservesleutels en een schriftelijk overzicht van elke codecombinatie; 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 dienen hetzelfde beschermingsniveau te krijgen als het materiaal waartoe zij toegang verschaffen.

13. De kennis omtrent de codecombinaties van beveiligingsopbergmiddelen wordt beperkt tot een zo klein mogelijke kring. 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 ten minste om de twaalf maanden.

Indringerdetectie-/signaleringssystemen

14. 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 continue werking van het systeem te waarborgen wanneer de hoofdelektriciteitsvoorziening uitvalt. Een andere fundamentele eis 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.

Goedgekeurde uitrusting

15. De NVI zal op basis van eigen of bilaterale bronnen lijsten bijhouden van het type en model van de beveiligingsuitrusting die zij hebben goedgekeurd voor de directe of indirecte bescherming van gerubriceerde gegevens onder diverse gespecificeerde omstandigheden en voorwaarden. De dienst beveiliging van het SGR zal een soortgelijke lijst bijhouden, die onder meer is gebaseerd op informatie van de NVI's. Gedecentraliseerde EU-organen dienen met de Dienst beveiliging van het SGR en, waar passend, met de NVI van de gastlidstaat te overleggen voordat zij een dergelijke uitrusting aankopen.

Fysieke bescherming van kopieermachines en faxapparaten

16. Kopieermachines en faxapparaten worden fysiek beschermd om te waarborgen dat zij alleen door gemachtigde personen kunnen worden gebruikt, en dat alle gerubriceerde producten de passende controles ondergaan.

BESCHERMING TEGEN WAARNEMING VAN BUITENAF EN AFLUISTEREN

Waarneming van buitenaf

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

Afluisteren

18. Kantoren of zones waar regelmatig als 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 beveiligingsinstantie, waar nodig na overleg met de NVI's.

19. Om te bepalen welke beschermende maatregelen moeten worden genomen op locaties 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 de Dienst beveiliging van het SGR deskundigen van NVI's om bijstand vragen. Veiligheidsfunctionarissen van gedecentraliseerde EU-organen kunnen de Dienst beveiliging van het SGR vragen technische inspecties uit te voeren, en/of deskundigen van NVI's om bijstand vragen.

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

TECHNISCH VEILIGE ZONES

21. 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.

22. Voor controledoeleinden zal een uitvoerige lijst van installaties en meubilair worden bijgehouden. Meubelstukken of apparatuur worden niet in een dergelijke zone binnengebracht dan nadat zij door speciaal opgeleid veiligheidspersoneel zijn onderworpen aan een zorgvuldige inspectie die mogelijke afluisterapparatuur op het spoor moet komen. In het algemeen moet de installatie van communicatielijnen in technisch veilige zones worden vermeden.

AFDELING V

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

1. Toegang tot gerubriceerde EU-gegevens zal slechts worden verleend aan personen die een „need-to-know" hebben d.w.z. in verband met de uitvoering van hun opdrachten of missies van gerubriceerde EU-gegevens moeten kennisnemen. Toegang tot als TRÈS SECRET UE/EU TOP SECRET, SECRET UE en CONFIDENTIEL UE gerubriceerde gegevens zal alleen worden verleend aan personen die in het bezit zijn van de passende veiligheidsmachtiging.

2. De verantwoordelijkheid om overeenkomstig de taakvereisten te bepalen wie een „need-to-know" heeft, berust bij het SGR, de gedecentraliseerde EU-organen en de dienst of afdeling van de lidstaat waar de betrokkene in dienst zal worden genomen.

3. De verantwoordelijkheid voor het veiligheidsonderzoek van het personeel berust bij de werkgever van de ambtenaar, die zich daarbij baseert op de relevante, van toepassing zijnde procedures. Wat de ambtenaren en andere personeelsleden van het SGR betreft, voorziet afdeling VI in de procedure voor veiligheidsmachtiging.

   Deze 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.

4. Diegenen die geen ambtenaren of andere personeelsleden van het SGR of van de lidstaten zijn, bijvoorbeeld leden, ambtenaren of andere personeelsleden van de Instellingen van de EU, met wie noodzakelijkerwijs gerubriceerde EU-gegevens moeten worden besproken, of aan wie deze moeten worden getoond, dienen een veiligheidsmachtiging te hebben voor wat betreft gerubriceerde EU-gegevens, en instructies te hebben omtrent hun verantwoordelijkheid vanuit veiligheidsoogpunt. Dezelfde regel geldt in soortgelijke omstandigheden voor externe contractanten, deskundigen of adviseurs.

SPECIFIEKE VOORSCHRIFTEN INZAKE DE TOEGANG TOT ALS TRES SECRET UE/ EU TOP SECRET GERUBRICEERDE GEGEVENS

5. Alle personen die toegang moeten hebben tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens dienen hiervoor eerst een veiligheidsonderzoek te ondergaan.

6. Alle personen van wie vereist is dat zij toegang hebben tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens moeten door het hoofd van hun afdeling worden aangewezen, en hun naam moet worden ingeschreven in het passende TRÈS SECRET UE/EU TOP SECRET-register.

7. Alvorens toegang te hebben tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens dienen alle personen een attest te ondertekenen waarin zij verklaren instructies te hebben ontvangen inzake de beveiligingsprocedures van de Raad, en ten volle hun speciale verantwoordelijkheid voor het waarborgen van de als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens te beseffen, alsook de gevolgen waarin de voorschriften van de EU en de nationale wettelijke of administratiefrechtelijke voorschriften voorzien wanneer gerubriceerde gegevens met opzet of door nalatigheid in handen van onbevoegden vallen.

8. Wanneer personen tijdens vergaderingen en dergelijke toegang hebben tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens, stelt de bevoegde controleambtenaar van de dienst of instantie waar die personen tewerk zijn gesteld, de organiserende instantie ervan in kennis dat de betrokkenen hiertoe gemachtigd zijn.

9. De namen van alle personen die niet langer taken vervullen waarvoor toegang tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens is vereist, worden verwijderd uit het TRÈS SECRET UE/EU TOP SECRET-register. Bovendien wordt de aandacht van al deze personen opnieuw gevestigd op hun speciale verantwoordelijkheid voor het waarborgen van de als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens. Tevens ondertekenen zij een verklaring dat zij de als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens die in hun bezit zijn, niet zullen gebruiken of doorgeven.

SPECIFIEKE VOORSCHRIFTEN BETREFFENDE DE TOEGANG TOT ALS SECRET UE EN CONFIDENTIEL UE GERUBRICEERDE GEGEVENS

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

11. Alle personen die toegang hebben tot als SECRET UE of CONFIDENTIEL UE gerubriceerde gegevens worden vertrouwd gemaakt met de passende beveiligingsvoorschriften en zijn zich bewust van de gevolgen van nalatigheid.

12. Wanneer personen tijdens vergaderingen en dergelijke toegang hebben tot als SECRET UE of CONFIDENTIEL UE gerubriceerde gegevens, stelt de bevoegde controleambtenaar van de dienst of instantie waar die personen tewerk zijn gesteld, de organiserende instantie ervan in kennis dat de betrokkenen hiertoe gemachtigd zijn.

SPECIFIEKE VOORSCHRIFTEN BETREFFENDE DE TOEGANG TOT ALS RESTREINT UE GERUBRICEERDE GEGEVENS

13. Personen die toegang hebben tot als RESTREINT UE gerubriceerde gegevens worden geïnformeerd door de relevante beveiligingsvoorschriften van de Raad en de gevolgen van nalatigheid.

OVERDRACHTEN

14. Wanneer een personeelslid wordt overgeplaatst uit een ambt dat de verwerking van gerubriceerd EU-materiaal inhoudt, houdt het register toezicht op de juiste overdracht van dat materiaal van de vertrekkende ambtenaar naar zijn opvolger.

SPECIALE INSTRUCTIES

15. Personen die gerubriceerde EU-gegevens moeten verwerken, dienen bij het aanvaarden van hun functie en vervolgens op gezette tijden instructies te krijgen betreffende:

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

    b) de voorzorgsmaatregelen die zij moeten treffen in hun betrekkingen met de pers;

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

    d) de verplichting aan de relevante beveiligingsinstanties 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 beveiliging.

16. 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, ontvangen instructies betreffende de technieken waarvan bekend is dat zij door diverse inlichtingendiensten worden gebruikt.

17. Voor personen die met goed gevolg een veiligheidsonderzoek hebben ondergaan inzake toegang tot gerubriceerde EU-gegevens bestaan geen beveiligingsvoorschriften met betrekking tot privéreizen naar welke bestemming dan ook. De bevoegde beveiligingsinstanties zullen de ambtenaren en andere personeelsleden die onder hun verantwoordelijkheid vallen echter vertrouwd maken met eventueel voor hen geldende reisvoorschriften. Het valt onder de verantwoordelijkheid van de beveiligingsambtenaren om voor de personeelsleden bijeenkomsten te organiseren waar zij hun kennis inzake deze speciale instructies kunnen opfrissen.

AFDELING VI

PROCEDURE MET BETREKKING TOT HET VEILIGHEIDSONDERZOEK VOOR AMBTENAREN EN ANDERE PERSONEELSLEDEN VAN HET SGR

1. Alleen ambtenaren en andere personeelsleden van het SGR of personen die daar werken en die, uit hoofde van hun plichten de eisen van de dienst kennis moeten nemen of gebruik moeten maken van bij de Raad bewaarde gerubriceerde gegevens, hebben toegang tot dergelijke gegevens.

2. Om toegang te hebben tot als TRÈS SECRET UE/EU TOP SECRET, SECRET UE en CONFIDENTIEL UE gerubriceerde gegevens, moeten de personen waarnaar in punt 1 wordt verwezen, gemachtigd zijn overeenkomstig de procedure van de punten 4 en 5.

3. Machtiging wordt alleen verleend aan personen die met goed gevolg een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten, (NVI's) om overeenkomstig de procedure van de punten 6 tot en met 10 hebben ondergaan.

4. Het tot aanstelling bevoegd gezag in de zin van artikel 2, alinea 1 van het ambtenarenstatuut, is verantwoordelijk voor het verlenen van de machtigingen waarnaar wordt verwezen in de punten 1, 2 en 3.

   Het tot aanstelling bevoegd gezag verleent machtiging na het advies te hebben ingewonnen van de bevoegde nationale instanties van de lidstaten, die zulks uitbrengen op basis van het veiligheidsonderzoek dat overeenkomstig de punten 6 tot en met 12 wordt uitgevoerd.

5. De machtiging, die geldig is voor een periode van vijf jaar, mag de duur van de functie op grond waarvan de machtiging is verleend, niet overschrijden. Zij kan overeenkomstig de procedure van punt 4, door het tot aanstelling bevoegd gezag worden verlengd.

   Een machtiging kan door het tot aanstelling bevoegd gezag worden ingetrokken, wanneer het meent dat hiervoor te rechtvaardigen gronden aanwezig zijn. Van een besluit tot intrekking van de machtiging wordt kennis gegeven aan de betrokkene, die mag verzoeken door het tot aanstelling bevoegd gezag te worden gehoord, en aan de bevoegde nationale instantie.

6. Het doel van het veiligheidsonderzoek is vast te stellen dat er geen bezwaar tegen is dat de betrokkene toegang heeft tot gerubriceerde gegevens die door de Raad worden bewaard.

7. Een veiligheidsonderzoek wordt met behulp van de betrokkene en op verzoek van het tot aanstelling bevoegd gezag uitgevoerd door de bevoegde nationale instanties van de lidstaat waarvan de te onderzoeken persoon onderdaan is. Mocht de betrokkene op het grondgebied van een andere lidstaat wonen, dan kunnen de nationale instanties de samenwerking van de instanties van de staat van verblijf verkrijgen.

8. Bij wijze van onderdeel van het veiligheidsonderzoek wordt de betrokkene verzocht een formulier in te vullen waarin hem naar zijn persoonlijke gegevens wordt gevraagd.

9. Het tot aanstelling bevoegd gezag specificeert in zijn verzoek het type en het niveau van de gerubriceerde gegevens die aan de betrokkene ter beschikking moeten worden gesteld, zodat de bevoegde nationale instanties het veiligheidsonderzoek kunnen uitvoeren, en hun advies kunnen geven omtrent de machtigingsgrond die bij de betrokkene past.

10. Het gehele veiligheidsonderzoek is, samen met het verkregen resultaat, onderworpen aan de terzake vigerende voorschriften in de betrokken lidstaat, ook die betreffende de mogelijkheid tot beroep.

11. Wanneer de bevoegde nationale instanties van de lidstaat een positief advies uitbrengen, kan het tot aanstelling bevoegd gezag de betrokkene machtiging verlenen.

12. Van een negatief advies van de bevoegde nationale instanties wordt kennis gegeven aan de betrokkene, die mag verzoeken te worden gehoord door het tot aanstelling bevoegd gezag. Wanneer dit gezag het nodig acht, kan het de bevoegde nationale instanties vragen om, waar mogelijk, opheldering te verschaffen. Indien het negatief advies wordt bevestigd, wordt geen machtiging verleend.

13. Alle personen aan wie machtiging wordt verleend in de zin van de punten 4 en 5, 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.

14. Het tot aanstelling bevoegd gezag 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.

15. Bij wijze van uitzondering mag het tot aanstelling bevoegd gezag wanneer de dienst zulks vereist, nadat het 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 7 wordt verwezen, tijdelijke machtiging verlenen voor een periode van hoogstens zes maanden.

16. De voorlopige en tijdelijke machtigingen die aldus worden verleend, geven geen toegang tot als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens; deze toegang blijft beperkt tot ambtenaren die daadwerkelijk, overeenkomstig punt 7, met goed gevolg het veiligheidsonderzoek hebben ondergaan. Hangende het resultaat van dit onderzoek mag aan ambtenaren voor wie de machtigingsgraad TRÈS 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 SECRET UE.

AFDELING VII

VERVAARDIGING, VERSPREIDING, OVERDRACHT, OPSLAG EN VERNIETIGING VAN GERUBRICEERD EU-MATERIAAL

Inhoud

Algemene bepalingen

Deze afdeling bevat een beschrijving van de maatregelen voor de vervaardiging, verspreiding, overdracht, opslag en vernietiging van gerubriceerde EU-documenten als gedefinieerd in punt 3 a) van de grondbeginselen en minimumnormen voor de beveiliging in deel I van deze bijlage. Dit zal gebruikt worden als uitgangspunt voor de aanpassing van vergelijkbare maatregelen voor ander gerubriceerd EU-materiaal, per soort en per geval bekeken.

Hoofdstuk I

Vervaardiging en verspreiding van gerubriceerde EU-documenten

VERVAARDIGING

1. De EU-rubriceringen en -markeringen moeten overeenkomstig afdeling II worden vastgesteld en midden bovenaan en midden onderaan elke bladzijde worden vermeld; elke bladzijde wordt genummerd. Elk gerubriceerd EU-document krijgt een referentienummer en een datum. Bij TRÈS SECRET UE/EU TOP SECRET- en SECRET UE-documenten wordt het referentienummer op elke bladzijde vermeld. 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 van als CONFIDENTIEL UE en hoger gerubriceerde documenten vermeld.

2. Als CONFIDENTIEL UE en hoger gerubriceerde documenten mogen alleen getypt, vertaald, opgeslagen, gefotokopieerd, magnetisch gereproduceerd of op microfilm gezet worden door personen die ten minste voor de betrokken rubriceringsgraad van het document in kwestie, machtiging voor toegang tot gerubriceerde EU-gegevens hebben, behalve in het speciale geval dat in punt 31 van deze afdeling beschreven wordt.

   De bepalingen voor de productie van gerubriceerde documenten met computers staan in afdeling XI.

VERSPREIDING

3. Gerubriceerde EU-gegevens mogen alleen op een „need to know"-basis, verspreid worden onder personen, die een passende veiligheidsmachtiging hebben. De initiële verspreiding wordt gespecificeerd door de instantie waarvan de documenten afkomstig zijn.

4. TRÈS SECRET UE/EU TOP SECRET-documenten worden verspreid via de TRÈS SECRET UE/EU TOP SECRET-registers (zie afdeling VIII). Voor TRÈS SECRET UE/EU TOP SECRET-berichten kan het bevoegde register het hoofd van het communicatiecentrum toestemming geven het aantal kopieën te maken dat in de lijst van de geadresseerden vermeld is.

5. Als SECRET UE en lager gerubriceerde documenten kunnen door de oorspronkelijke geadresseerde op „need-to-know"-basis doorgezonden worden aan andere geadresseerden. De instanties waarvan het document afkomstig is moeten eventuele waarschuwingsmarkeringen echter duidelijk aangeven. In geval van dergelijke waarschuwingsmarkeringen mag de geadresseerde documenten alleen doorzenden met toestemming van de instanties waarvan de documenten afkomstig zijn.

6. Als CONFIDENTIEL UE en hoge gerubriceerde documenten worden bij aankomst in of vertrek uit een gebouw in het register van dat gebouw genoteerd. Met de bijzonderheden (referenties, datum en, indien van toepassing, het kopienummer) moeten de documenten geïdentificeerd kunnen worden; die gegevens worden in een logboek of een speciaal beveiligd computermedium ingevoerd.

Hoofdstuk II

Overdracht van gerubriceerde EU-documenten

VERPAKKING

7. Als CONFIDENTIEL UE en hoge gerubriceerde documenten worden in stevige, ondoorzichtige dubbele dienstenveloppen vervoerd. De binnenenveloppe wordt gemerkt met de toepasselijke EU-rubriceringsgraad en, zo mogelijk, de nodige gegevens over functie, titel en adres van de ontvanger.

8. Alleen een controlefunctionaris van het register of zijn plaatsvervanger mag de binnenenveloppe openen en voor ontvangst van de ingesloten documenten tekenen, tenzij de enveloppe geadresseerd is aan een welbepaalde persoon. In dat geval wordt in het register de aankomst van de enveloppe genoteerd, en mag alleen de persoon aan wie de enveloppe geadresseerd is de binnenenveloppe openen en tekenen voor ontvangst van de daarin ingesloten documenten.

9. In de binnenenveloppe wordt een ontvangstbewijs ingesloten. Op dat bewijs, dat niet gerubriceerd wordt, staan het referentienummer, de datum en het kopienummer van het document, maar nooit het onderwerp.

10. De binnenenveloppe wordt in een andere buitenenveloppe ingesloten, waarop een paknummer voor de ontvangstregistratie wordt aangebracht. In geen enkel geval mag op de buitenenveloppe de rubriceringsgraad vermeld staan.

11. Voor als CONFIDENTIEL UE en hoger gerubriceerde documenten krijgen koeriers en boodschappers een ontvangstbewijs dat gerelateerd is aan het paknummer.

OVERDRACHT BINNEN EEN GEBOUW OF EEN GROEP GEBOUWEN

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

OVERDRACHT VAN EU-DOCUMENTEN BINNEN EEN LAND

13. Binnen een land mogen TRÈS SECRET UE/EU TOP SECRET-documenten alleen verzonden worden met behulp van een officiële koeriersdienst of door personen die gemachtigd zijn om toegang te hebben tot TRÈS SECRET UE/EU TOP SECRET-gegevens.

14. Wanneer er een koeriersdienst gebruikt wordt voor de overdracht van een TRÈS SECRET UE/EU TOP SECRET-document buiten een gebouw of groep gebouwen, moeten de verpakkings- en ontvangstbepalingen van dit hoofdstuk II nageleefd worden. Koeriersdiensten moeten zodanig bemand zijn dat pakketjes met TRÈS SECRET UE/EU TOP SECRET-documenten te allen tijde onder de directe supervisie van de verantwoordelijke functionaris blijven.

15. Bij wijze van uitzondering mogen TRÈS SECRET UE/EU TOP SECRET-documenten door andere functionarissen dan koeriers uit een gebouw of groep gebouwen meegenomen worden voor gebruik ter plaatse in vergaderingen en besprekingen, op voorwaarde dat

    a) die functionaris gemachtigd is om toegang te hebben tot die TRÈS SECRET UE/EU TOP SECRET-documenten;

    b) de wijze van vervoer voldoet aan de nationale voorschriften voor de overdracht van nationale TOP SECRET-documenten;

    c) de functionaris de TRÈS SECRET UE/EU TOP SECRET-documenten in geen geval onbeheerd laat;

    d) er een regeling getroffen wordt voor de lijst van de aldus vervoerde documenten die bijgehouden moet worden in het TRÈS SECRET UE/EU TOP SECRET-register dat die documenten bevat, in een logboek moet worden genoteerd, en bij terugkeer aan de hand van die gegevens moet worden gecontroleerd.

16. Binnen een land mogen SECRET UE- en CONFIDENTIEL UE-documenten per post worden verzonden, indien de nationale regelgeving dat toestaat en die regelgeving wordt nageleefd, of via een koeriersdienst dan wel door personen die gemachtigd zijn om toegang te hebben tot de gerubriceerde EU-gegevens.

17. Elke lidstaat of gedecentraliseerd EU-orgaan moet voor het personeel dat gerubriceerde EU-documenten vervoert instructies opstellen die op deze voorschriften gebaseerd zijn. De drager dient die instructies te lezen en te ondertekenen. In het bijzonder moet in die instructies worden aangegeven dat de documenten in geen geval:

    a) door de drager uit handen mogen worden gegeven, tenzij voor veilige bewaring overeenkomstig afdeling IV;

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

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

OVERDRACHT TUSSEN LIDSTATEN

18. Als CONFIDENTIEL UE en hoger gerubriceerd materiaal moet door diplomatieke of militaire koeriersdiensten van de ene lidstaat naar de andere worden gebracht.

19. Persoonlijk vervoer van als SECRET UE of CONFIDENTIEL UE gerubriceerd materiaal mag echter worden toegestaan, als daartoe voorzorgsmaatregelen genomen worden, zodat het materiaal niet in handen van onbevoegden valt.

20. De NVI's kunnen persoonlijk vervoer toestaan wanneer er geen diplomatieke of militaire koeriers beschikbaar zijn, of wanneer het gebruik van dergelijke koeriers een vertraging zou opleveren die schadelijk is voor de EU-operaties en de beoogde geadresseerde het materiaal dringend nodig heeft. Elke lidstaat moet instructies opstellen voor het persoonlijk internationaal vervoer van materiaal tot en met de rubriceringsgraad op SECRET UE door andere personen dan diplomatieke of militaire koeriers. Die instructies moeten het volgende voorschrijven:

a) de drager heeft de passende veiligheidsmachtiging die door de lidstaten is toegekend;

b) in het betrokken bureau of register wordt een bestand bijgehouden van al het materiaal dat op die wijze vervoerd wordt;

c) pakketten of tassen met EU-materiaal zijn voorzien van een officieel stempel ter voorkoming van douanecontroles, en van etiketten met identificatiegegevens en instructies voor de eventuele vinder;

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

e) in geval van vervoer over land mag niet over het grondgebied van een niet-EU-lidstaat worden gereisd of mag de grens daarvan niet overschreden worden, tenzij deze de lidstaat van verzending een speciale garantie heeft geboden;

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

g) de drager mag het materiaal niet uit handen geven, tenzij het overeenkomstig de bepalingen voor veilige bewaring van afdeling IV wordt opgeslagen;

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) als het materiaal documenten bevat, mogen deze niet op openbare plaatsen (b.v. vliegtuigen, treinen, enz.) gelezen worden.

De persoon die met het vervoer van het gerubriceerd materiaal belast is, moet na lezing een veiligheidscertificaat ondertekenen dat tenminste de bovenbedoelde instructies bevat alsmede de procedures die in een noodgeval gevolgd moeten worden of indien het pakket met het gerubriceerde materiaal door de douane of de veiligheidsdienst van een luchthaven wordt opgeëist.

OVERDRACHT VAN ALS RESTREINT UE GERUBRICEERDE EU-DOCUMENTEN

21. Voor het vervoer van als RESTREINT UE gerubriceerde EU-documenten zijn geen speciale bepalingen vastgesteld, behalve dat ervoor gezorgd moet worden dat die documenten niet in handen van onbevoegden vallen.

VEILIGHEIDSONDERZOEK VAN KOERIERS

22. Alle koeriers en boodschappers die ingezet worden om SECRET UE- en CONFIDENTIEL UE-documenten te vervoeren, moeten vooraf een passend veiligheidsonderzoek ondergaan.

Hoofdstuk III

Elektrische en andere middelen van technische overdracht

23. Er moeten communicatiebeveiligingsmaatregelen getroffen worden voor een beveiligde overdracht van gerubriceerde EU-gegevens. De voorschriften voor de overdracht van dergelijke gegevens staan in afdeling XI.

24. Alleen geaccrediteerde communicatiecentra en -netwerken en/of -terminals en -systemen mogen als CONFIDENTIEL UE of SECRET UE gerubriceerde gegevens doorzenden.

Hoofdstuk IV

Extra kopieën en vertalingen van en uittreksels uit gerubriceerde EU-documenten

25. Alleen de instantie die de documenten verstrekt heeft, mag toestemming geven voor het kopiëren of vertalen van TRÈS SECRET UE/EU TOP SECRET-documenten.

26. Wanneer personen zonder TRÈS SECRET UE/EU TOP SECRET-machtiging gegevens uit een TRÈS SECRET UE/EU TOP SECRET-document opvragen die zelf echter een andere rubricering hebben, kan aan het hoofd van het TRÈS SECRET UE/EU TOP SECRET-register worden toegestaan om het gevraagde aantal uittreksels uit dat document te leveren. Daarbij neemt het hoofd de nodige maatregelen om ervoor te zorgen dat die uittreksels de passende rubriceringsgraad krijgen.

27. Als SECRET UE en lager gerubriceerde documenten mogen door de geadresseerde gereproduceerd en vertaald worden met inachtneming van de nationale beveiligingsvoorschriften, op voorwaarde dat het „need-to-know"-beginsel strikt in acht wordt genomen. De beveiligingsmaatregelen die voor het originele document gelden, zijn ook van toepassing op de reproducties en/of vertalingen daarvan. De gedecentraliseerde EU-organen dienen de beveiligingsvoorschriften van de Raad toe te passen.

Hoofdstuk V

Verzamelen, controleren, opslaan en vernietigen van gerubriceerde EU-documenten

VERZAMELEN EN CONTROLEREN

28. Ieder jaar maakt elk TRÈS SECRET UE/EU TOP SECRET-register als bedoeld in afdeling VIII een gespecificeerd overzicht naar TRÈS SECRET UE/EU TOP SECRET-documenten overeenkomstig de bepalingen van afdeling VIII, punten 9 tot en met 11. EU-documenten die lager dan TRÈS SECRET UE/EU TOP SECRET gerubriceerd zijn, worden overeenkomstig de nationale richtsnoeren aan interne controles onderworpen; voor het SGR en de gedecentraliseerde EU-organen moet dat volgens de instructies van de secretaris-generaal/hoge vertegenwoordiger gebeuren.

Deze controle biedt de gelegenheid om opnieuw een standpunt te bepalen met betrekking tot

a) de mogelijkheid om bepaalde documenten lager te rubriceren of te derubriceren;

b) de vraag of bepaalde documenten vernietigd moeten worden.

ARCHIVERING VAN GERUBRICEERDE EU-GEGEVENS

29. Ter voorkoming van opslagproblemen krijgen de controlefunctionarissen van alle registers de toestemming om TRÈS SECRET UE/EU TOP SECRET-, SECRET UE- en CONFIDENTIEL UE-documenten op microfilm of met behulp van magnetische of optische middelen voor archiveringsdoeleinden vast te leggen, onder de volgende voorwaarden:

a) het vastleggen op en opslaan van microfilms wordt gedaan door personeelsleden die voor de desbetreffende rubriceringsgraad gemachtigd zijn;

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

c) de instantie die de documenten heeft verstrekt wordt ervan in kennis gesteld als er een TRÈS SECRET UE/EU TOP SECRET-document op microfilm vastgelegd/opgeslagen wordt;

d) een filmrolletje of een andere gegevensdrager mag alleen documenten bevatten met dezelfde TRÈS SECRET UE/EU TOP SECRET-, SECRET UE- of CONFIDENTIEL UE-rubricering;

e) TRÈS SECRET UE/EU TOP SECRET- of SECRET UE-documenten die op microfilm vastgelegd/opgeslagen zijn, worden duidelijk aangegeven in het logboek dat voor de jaarlijkse inventaris gebruikt wordt;

f) de originele documenten die op microfilm vastgelegd of anderszins opgeslagen zijn, worden volgens de voorschriften van de punten 31 tot en met 36 vernietigd.

30. Deze voorschriften zijn ook van toepassing op eventuele andere vormen van opslag die door de nationale veiligheidsinstanties zijn toegestaan, zoals elektromagnetische middelen en optische schijven.

ROUTINEVERNIETIGING VAN GERUBRICEERDE EU-DOCUMENTEN

31. Ter voorkoming van een onnodige opeenhoping van gerubriceerde EU-documenten, worden de documenten die door het hoofd van de dienst die ze bewaart, als achterhaald en overtollig worden beschouwd, zo spoedig mogelijk op onderstaande wijze vernietigd:

a) TRÈS SECRET UE/EU TOP SECRET-documenten mogen alleen vernietigd worden door het centrale register dat voor die documenten verantwoordelijk is. Elk vernietigd document wordt genoteerd in een proces-verbaal van vernietiging dat ondertekend wordt door de TRÈS SECRET UE/EU TOP SECRET-controlefunctionaris en de functionaris die getuige is bij de vernietiging en voor de TRÈS SECRET UE/EU TOP SECRET-graad gemachtigd is. 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 zullen er kopieën verstrekt worden aan de instantie waarvan de documenten afkomstig zijn of aan het betrokken centrale register.

c) TRÈS SECRET UE/EU TOP SECRET-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van TRÈS SECRET UE/EU TOP SECRET-documenten, zoals kladversies, ontwerpteksten, getypte aantekeningen en carbonpapier, worden onder toezicht van een TRÈS SECRET UE/EU TOP SECRET-functionaris vernietigd door verbranding, verpulping, versnippering of een andere methode waardoor de documenten onherkenbaar en onherstelbaar vernietigd worden.

32. SECRET UE-documenten worden vernietigd door het register dat voor die documenten verantwoordelijk is, onder toezicht van een persoon met een veiligheidsmachtiging, waarbij een van de in punt 31, onder c), genoemde procédés gebruikt wordt. Vernietigde SECRET UE-documenten worden genoteerd op een ondertekend proces-verbaal van vernietiging dat door het register, samen met de verspreidingsformulieren, gedurende ten minste drie jaar bewaard worden.

33. CONFIDENTIEL UE-documenten worden vernietigd door het register dat voor die documenten verantwoordelijk is, onder toezicht van een persoon met een veiligheidsmachtiging, waarbij een van de in punt 31, onder c), genoemde procédés gebruikt wordt. De vernietigde documenten worden genoteerd overeenkomstig de nationale voorschriften of, in het geval van het SGR of gedecentraliseerde EU-organen, volgens de instructies van de secretaris-generaal/ hoge vertegenwoordiger.

34. RESTREINT UE-documenten worden vernietigd door het register dat voor die documenten verantwoordelijk is of door de gebruiker overeenkomstig de nationale voorschriften of, in het geval van het SGR of gedecentraliseerde EU-organen, volgens de instructies van de secretaris-generaal/hoge vertegenwoordiger.

VERNIETIGING IN NOODGEVALLEN

35. Het SGR, de lidstaten en de gedecentraliseerde EU-organen moeten op de plaatselijke omstandigheden gebaseerde plannen opstellen ter beveiliging van gerubriceerd EU-materiaal in crisissituaties, zonodig met inbegrip van noodvernietigings- en evacuatieplannen; deze bepalen voor de respectieve organisaties de instructies die nodig geacht worden om te voorkomen dat gerubriceerde EU-gegevens in handen van onbevoegden vallen.

36. De regeling voor het beveiligen en/of vernietigen van SECRET UE- en CONFIDENTIEL UE-materiaal in crisissituaties mag in geen geval ten koste gaan van het beveiligen of vernietigen van TRÈS SECRET UE/EU TOP SECRET-materiaal, met inbegrip van de encryptieapparatuur, waarvan de werking voorrang heeft op alle andere taken. De maatregelen voor de beveiliging en vernietiging van encryptieapparatuur in noodsituaties worden op grond van ad hoc instructies vastgesteld.

Hoofdstuk VI

Specifieke voorschriften voor raadsdocumenten

37. Binnen het secretariaat-generaal van de Raad zal een „bureau voor gerubriceerde gegevens" toezicht houden op de als SECRET UE of CONFIDENTIEL UE gerubriceerde gegevens in Raadsdocumenten.

Het bureau heeft, onder toezicht van de directeur-generaal voor personeel en administratie, de volgende taken:

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

d) het opstellen, in samenwerking met de Dienst beveiliging, van praktische regelingen voor het rubriceren en derubriceren van gegevens.

38. Het bureau voor gerubriceerde gegevens houdt een register bij met daarin vermeld:

a) de datum van opstelling van de gerubriceerde gegevens;

b) het rubriceringsniveau;

c) de datum waarop de rubricering verstrijkt;

d) naam en werkadres van de afzender;

e) de opbergmiddelen, met volgnummer;

f) het onderwerp;

g) het aantal;

h) het aantal verspreide kopieën;

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

j) een register van het derubriceren en lager rubriceren van gerubriceerde gegevens.

39. De algemene voorschriften van de hoofdstukken I tot en met V van deze afdeling zijn ook van toepassing op het bureau voor gerubriceerde gegevens van het SGR, tenzij in dit hoofdstuk specifieke voorschriften zijn vastgesteld.

AFDELING VIII

EU TOP SECRET-REGISTERS

1. De TRÈS SECRET UE/EU TOP SECRET-registers zijn bedoeld voor het registreren, verwerken en verspreiden van TRÈS SECRET UE/EU TOP SECRET-documenten overeenkomstig de beveiligingsvoorschriften. Hoofd van het TRÈS SECRET UE/EU TOP SECRET-register in elke lidstaat, op het SGR en, in voorkomend geval, in de gedecentraliseerde EU-organen, is de TRÈS SECRET UE/EU TOP SECRET-controlefunctionaris.

2. De centrale registers handelen op dezelfde wijze als de belangrijkste autoriteit van ontvangst en verzending in de lidstaten, het SGR en de gedecentraliseerde EU-organen waarin dergelijke registers zijn opgezet, alsmede, indien van toepassing, in andere EU-instellingen, internationale organisaties en derde landen waarmee de Raad overeenkomsten heeft gesloten inzake beveiligingsprocedures voor de uitwisseling van gerubriceerde gegevens.

3. Indien nodig worden er subregisters opgezet voor het intern beheer van TRÈS SECRET UE/EU TOP SECRET-documenten; hierin wordt bijgehouden waar elk document waarvoor het subregister verantwoordelijk is, zich bevindt.

4. TRÈS SECRET UE/EU TOP SECRET-subregisters worden overeenkomstig afdeling I opgezet voor de lange termijn, en gekoppeld aan een centraal TRÈS SECRET UE/EU TOP SECRET-register. Indien de TRÈS SECRET UE/EU TOP SECRET-documenten slechts tijdelijk en incidenteel geraadpleegd moeten worden, kunnen deze vrijgegeven worden zonder dat er een TRÈS SECRET UE/EU TOP SECRET-subregister wordt opgezet, op voorwaarde dat er maatregelen worden getroffen om ervoor te zorgen dat zij onder de controle van het betrokken TRÈS SECRET UE/EU TOP SECRET-register blijven en alle voorschriften inzake fysieke en personeelsgerelateerde beveiliging nageleefd worden.

5. Subregisters mogen geen TRÈS SECRET UE/EU TOP SECRET-documenten rechtstreeks overdragen aan andere subregisters van hetzelfde centrale TRÈS SECRET UE/EU TOP SECRET-register zonder uitdrukkelijke toestemming van laatstgenoemde instantie.

6. Elke uitwisseling van TRÈS SECRET UE/EU TOP SECRET-documenten tussen subregisters die niet tot hetzelfde centrale register behoren, verloopt via de centrale TRÈS SECRET UE/EU TOP SECRET-registers.

CENTRALE EU TOP SECRET-REGISTERS

7. Evenals de controlefunctionaris is het hoofd van een centraal TRÈS SECRET UE/EU TOP SECRET-register verantwoordelijk voor:

   a) de overdracht van TRÈS SECRET UE/EU TOP SECRET-documenten overeenkomstig de voorschriften van afdeling VII;

   b) het bijhouden van een lijst van al zijn TRÈS SECRET UE/EU TOP SECRET-subregisters, alsmede de naam en de handtekening van de aangewezen controlefunctionarissen en hun gemachtigde plaatsvervangers;

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

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

   e) het bijhouden van een lijst van alle centrale TRÈS SECRET UE/EU TOP SECRET-registers waarmee hij normaliter correspondeert, alsmede de naam en de handtekening van de aangewezen controlefunctionarissen en hun gemachtigde plaatsvervangers;

   f) de fysieke bewaking van alle TRÈS SECRET UE/EU TOP SECRET-documenten die volgens de voorschriften van afdeling IV in het register bewaard worden.

TRÈS SECRET UE/EU TOP SECRET-SUBREGISTERS

8. Evenals de controlefunctionaris is het hoofd van een TRÈS SECRET UE/EU TOP SECRET-subregister verantwoordelijk voor:

   a) de overdracht van TRÈS SECRET UE/EU TOP SECRET-documenten overeenkomstig de voorschriften van afdeling VII en afdeling VIII, punten 5 en 6;

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

c) de verspreiding van TRÈS 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 hij is nagegaan of de geadresseerde de vereiste veiligheidsmachtiging heeft;

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

e) het bijhouden van een lijst van TRÈS SECRET UE/EU TOP SECRET-registers waarmee hij TRÈS SECRET UE/EU TOP SECRET-documenten mag uitwisselen, alsmede de naam en de handtekening van de controlefunctionarissen daarvan en hun gemachtigde plaatsvervangers;

f) de fysieke bewaking van alle TRÈS SECRET UE/EU TOP SECRET-documenten die volgens de voorschriften van afdeling IV in het subregister bewaard worden.

INVENTARIS

9. Ieder jaar stelt elk TRÈS SECRET UE/EU TOP SECRET-register een gespecificeerde inventaris op van alle TRÈS SECRET UE/EU TOP SECRET-documenten waarvoor het verantwoordelijk is. Het register wordt geacht verantwoordelijk te zijn voor een document wanneer dat zich fysiek op het register bevindt, of wanneer het register een ontvangstbewijs heeft van het TRÈS SECRET UE/EU TOP SECRET-register waaraan het document is overgedragen, dan wel een proces-verbaal van vernietiging voor het document of een opdracht om dat document lager te rubriceren of te derubriceren.

10. Subregisters zenden de bevindingen van hun jaarlijkse inventaris toe aan het centraal register waaronder zij ressorteren, op een tijdstip dat door het centraal register bepaald wordt.

11. De nationale veiligheidsinstanties, alsmede de EU-instellingen, internationale organisaties en gedecentraliseerde EU-organen die een centraal TRÈS SECRET UE/EU TOP SECRET-register hebben opgezet, zenden de bevindingen van de jaarlijkse inventaris van de centrale TRÈS SECRET UE/EU TOP SECRET-registers elk jaar uiterlijk op 1 april toe aan de secretaris-generaal/hoge vertegenwoordiger.

AFDELING IX

TOE TE PASSEN BEVEILIGINGSMAATREGELEN INDIEN VERGADERINGEN OVER ZEER GEVOELIGE AANGELEGENHEDEN BUITEN GEBOUWEN VAN DE RAAD WORDEN GEHOUDEN

ALGEMEEN

1. Indien bijeenkomsten van de Europese Raad, zittingen van de Raad, ministeriële of andere belangrijke vergaderingen buiten de gebouwen van de Raad in Brussel en Luxemburg plaatsvinden en de bijzondere beveiligingseisen die voortvloeien uit de hoge gevoeligheid van de behandelde aangelegenheden of gegevens zulks rechtvaardigen, dienen de hieronder beschreven beveiligingsmaatregelen te worden getroffen. Deze maatregelen hebben alleen betrekking op de bescherming van gerubriceerde EU-gegevens; er moeten wellicht ook andere beveiligingsmaatregelen worden overwogen.

VERANTWOORDELIJKHEID

Gastlidstaten

2. De lidstaat op wiens grondgebied de vergadering plaatsvindt (de gastlidstaat), is samen met de Dienst beveiliging van het SGR verantwoordelijk voor de beveiliging van de bijeenkomsten van de Europese Raad, zittingen van de Raad, ministeriële of andere belangrijke vergaderingen alsook voor de fysieke veiligheid van de delegatieleiders en hun medewerkers.

Wat de beveiliging betreft, dient de gastlidstaat er in het bijzonder voor te zorgen dat:

a) een plan van aanpak wordt opgesteld voor beveiligingsrisico's en beveiligingsincidenten; de betreffende maatregelen slaan in het bijzonder op het veilig opbergen van gerubriceerde EU-documenten in kantoorruimten;

b) maatregelen worden getroffen om toegang te kunnen verlenen tot de communicatiesystemen van de Raad, teneinde gerubriceerde EU-berichten te kunnen ontvangen en versturen. De gastlidstaat stelt desgewenst beveiligde telefoonsystemen ter beschikking.

Lidstaten

3. De autoriteiten van de lidstaten dienen het nodige te doen om ervoor te zorgen dat:

a) hun nationale delegatieleden voorzien worden van de vereiste veiligheidsmachtiging, zo nodig per signaal of fax, hetzij direct aan de beveiligingsfunctionaris voor de vergadering, hetzij via de Dienst beveiliging van het SGR;

b) specifieke bedreigingen worden gemeld aan de autoriteiten van de gastlidstaat en in voorkomend geval aan de Dienst beveiliging van het SGR, zodat het nodige kan worden gedaan.

Beveiligingsfunctionaris voor de vergadering

4. Er dient een beveiligingsfunctionaris te worden aangewezen, die verantwoordelijk is voor de algemene voorbereiding van en het toezicht op de algemene interne beveiligingsmaatregelen, alsook voor de coördinatie met de andere betrokken veiligheidsinstanties. De maatregelen die de beveiligingsfunctionaris treft, dienen op hoofdlijnen het volgende in te houden:

a) i) beschermingsmaatregelen op de vergaderplaats, om ervoor te zorgen dat de vergadering kan plaatsvinden zonder incidenten die de beveiliging van gerubriceerde EU-gegevens die in de vergadering worden gebruikt, kunnen compromitteren;

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

iii) permanente coördinatie met de bevoegde autoriteiten van de gastlidstaat en met de Dienst beveiliging van het SGR;

b) beveiligingsinstructies opnemen in het vergaderdossier, met voldoende aandacht voor de in deze voorschriften neergelegde eisen en andere nodig geachte beveiligingsinstructies.

Dienst beveiliging van het SGR

5. De Dienst beveiliging van het SGR geeft beveiligingsadviezen bij de voorbereiding van de vergadering; de dienst is in de vergadering vertegenwoordigd en staat de beveiligingsfunctionaris voor de vergadering en de delegaties waar nodig met raad en daad bij.

6. Elke delegatie in de vergadering dient een beveiligingsfunctionaris aan te wijzen, die binnen zijn delegatie verantwoordelijk is voor beveiligingskwesties en in contact staat met de beveiligingsfunctionaris voor de vergadering en met de vertegenwoordiger van de Dienst beveiliging van het SGR, indien zulks nodig is.

BEVEILIGINGSMAATREGELEN

Beveiligingszones

7. De volgende beveiligingszones dienen te worden ingesteld:

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

   b) een beveiligingszone 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.

Pasjes

8. De beveiligingsfunctionaris voor de vergadering 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 beveiligingszones.

9. De beveiligingsinstructies 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 beveiligingspersoneel kunnen worden gecontroleerd.

10. Afgezien van de deelnemers die een pasje hebben mogen zo weinig mogelijk personen tot de vergaderlocatie worden toegelaten. Nationale delegaties die tijdens de vergadering bezoekers wensen te ontvangen, dienen de beveiligingsfunctionaris voor de vergadering daarvan in kennis te stellen. 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 die van de bezochte persoon. Bezoekers dienen te allen tijde te worden begeleid door beveiligingspersoneel 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 beveiligingspersoneel wanneer de bezoeker de vergaderlocatie verlaat.

Controle van foto- en audioapparatuur

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

Controle van aktetassen, draagbare computers en pakjes

12. Aktetassen en draagbare computers (alleen indien voorzien van een autonome energiebron) van houders van pasjes die toegang hebben tot een beveiligingszone, 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 beveiligingsfunctionaris van de betreffende delegatie, gescreend met speciale apparatuur of voor controle geopend door het beveiligingspersoneel. Indien de beveiligingsfunctionaris voor de vergadering zulks nodig acht, kunnen strengere maatregelen met betrekking tot de controle van aktetassen en pakjes worden vastgelegd.

Technische beveiliging

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

Documenten van delegaties

14. 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.

Veilig opbergen van documenten

15. Indien het SGR, 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 beveiligingsfunctionaris voor de vergadering overhandigen zodat deze functionaris de documenten conform goedgekeurde normen kan opbergen.

Controle van ruimten

16. De beveiligingsfunctionaris voor de vergadering dient erop toe te zien dat de ruimten van het SGR 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 de nodige maatregelen te treffen.

Verwijdering van afval van gerubriceerd EU-materiaal

17. Afval dient te worden behandeld als gerubriceerd EU-materiaal; aan het SGR en de delegaties dienen papiermanden of -zakken ter beschikking te worden gesteld om afval te verwijderen. Alvorens de hun toegewezen ruimten te verlaten, dienen het SGR en de delegaties hun afval aan de beveiligingsfunctionaris voor de vergadering te overhandigen, die ervoor zorgt dat het afval conform de beveiligingsvoorschriften wordt vernietigd.

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

AFDELING X

INBREUKEN OP DE BEVEILIGINGSVOORSCHRIFTEN EN COMPROMITTERING VAN GERUBRICEERDE EU-GEGEVENS

1. Een inbreuk op de beveiligingsvoorschriften is het resultaat van een handeling of een nalatigheid, in strijd met de geldende beveiligingsvoorschriften van de Raad of de nationale beveiligingsvoorschriften, die gerubriceerde EU-gegevens in gevaar kan brengen of compromitteren.

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

3. Gerubriceerde EU-gegevens kunnen gecompromitteerd zijn als resultaat 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.

4. Het is belangrijk dat eenieder die gerubriceerde EU-gegevens dient te verwerken, grondig wordt ingelicht over de beveiligingsprocedures, de gevaren van indiscretie en de betrekkingen met de pers. De betrokkenen dienen zich bewust te zijn van het belang dat elke inbreuk op de beveiligingsvoorschriften waarvan zij kennis krijgen, onverwijld aan de veiligheidsinstanties van de lidstaten, de instelling of het orgaan waarbij zij in dienst zijn wordt gemeld.

5. Indien een veiligheidsinstantie een inbreuk op de beveiligingsvoorschriften met betrekking tot gerubriceerde EU-gegevens dan wel het verlies of verdwijnen van gerubriceerd EU-materiaal ontdekt of daarvan in kennis wordt gesteld, doet zij tijdig het nodige om:

   a) de feiten vast te stellen;

   b) de aangerichte schade te beoordelen en te beperken;

   c) herhaling te voorkomen;

   d) de bevoegde instanties in kennis te stellen van de gevolgen van de inbreuk op de beveiligingsvoorschriften.

   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 dewelke de informatie aan compromittering was blootgesteld;

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

6. Zodra de veiligheidsinstanties kennis krijgen van een mogelijke inbreuk op de beveiligingsvoorschriften, dienen zij dit onmiddellijk te melden en daarbij de volgende procedure te volgen: het EU TOP SECRET-subregister doet melding via zijn centraal EU TOP SECRET-register aan de Dienst beveiliging van het SGR; indien gerubriceerde EU-gegevens binnen de jurisdictie van een lidstaat zijn gecompromitteerd, wordt dit op de in punt 5 gespecificeerde wijze aan de Dienst beveiliging van het SGR gemeld, via de verantwoordelijke persoon van de nationale veiligheidsinstantie.

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

8. Wanneer de secretaris-generaal/hoge vertegenwoordiger in kennis wordt gesteld van een inbreuk op de beveiligingsvoorschriften:

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

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

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

d) wordt hij 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. Verder dient verslag te worden uitgebracht van de schade aan belangen van de EU of van een of meer van haar lidstaten, alsmede van de stappen die zijn ondernomen om herhaling te voorkomen.

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

10. Eenieder die verantwoordelijk is voor het compromitteren van gerubriceerde EU-gegevens stelt zich bloot aan disciplinaire maatregelen, overeenkomstig de geldende regels en voorschriften. Een en ander laat een gerechtelijke actie onverlet.

AFDELING XI

BESCHERMING VAN GEGEVENS DIE VERWERKT WORDEN IN IT- EN COMMUNICATIESYSTEMEN

Inhoud

Hoofdstuk I

Inleiding

ALGEMEEN

1. Het beveiligingsbeleid en de beveiligingseisen in deze afdeling zijn van toepassing op alle communicatie- en informatiesystemen en netwerken (hierna SYSTEMEN genoemd) waarin als CONFIDENTIEL UE en hoger gerubriceerde gegevens worden verwerkt.

2. SYSTEMEN waarin als RESTREINT UE gerubriceerde gegevens worden verwerkt, behoeven beveiligingsmaatregelen om de vertrouwelijkheid van die gegevens te beschermen. Alle SYSTEMEN behoeven beveiligingsmaatregelen ter bescherming van hun integriteit en beschikbaarheid en van de gegevens die zij bevatten. De op die systemen toe te passen beveiligingsmaatregelen worden vastgesteld door de aangewezen instantie voor veiligheidsaccreditatie (IVA), zijn evenredig met het geschatte risico en sporen met het beleid zoals dat in deze beveiligingsvoorschriften is neergelegd.

3. De bescherming van sensorsystemen met ingebouwde IT-SYSTEMEN wordt bepaald en gespecificeerd in de algemene context van de systemen waarvan zij deel uitmaken; voorzover mogelijk worden daarbij de toepasselijke bepalingen van deze afdeling gehanteerd.

BEDREIGINGEN EN KWETSBAARHEDEN VAN SYSTEMEN

4. 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: vertrouwelijkheid, 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. Kwetsbaarheid kan bestaan in nalatigheid of kan verband houden met onvoldoende strenge, volledige of samenhangende controle; de kwetsbaarheid van systemen kan van technische, procedurele of operationele aard zijn.

5. 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 risico's 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. Deze SYSTEMEN vormen bijgevolg een aanlokkelijk doelwit voor spionage en sabotage, met name indien de daders vermoeden dat beveiligingsmaatregelen ondoeltreffend zijn.

BEVEILIGINGSMAATREGELEN

6. De in deze afdeling genoemde beveiligingsmaatregelen strekken er in de eerste plaats toe, bescherming te bieden tegen openbaarmaking zonder machtiging (verlies van vertrouwelijkheid) en verlies van integriteit en beschikbaarheid van gegevens. Om een afdoende beveiliging van een SYSTEEM waarin gerubriceerde EU-gegevens worden verwerkt, te kunnen verwezenlijken, worden de toepasselijke conventionele beveiligingsnormen gespecificeerd, samen met bijzondere beveiligingsprocedures en -technieken die op de respectieve SYSTEMEN zijn afgestemd.

7. Er wordt een evenwichtig geheel van beveiligingsmaatregelen opgesteld en uitgevoerd, met de bedoeling een veilige omgeving te creëren voor het functioneren van een SYSTEEM. Die maatregelen zijn van toepassing op fysieke elementen, personeel, niet-technische procedures, alsmede operationele computer- en communicatieprocedures.

8. Met het oog op de toepassing van het „need-to-know"-beginsel en teneinde openbaarmaking van gegevens zonder machtiging te voorkomen of op te sporen, moeten er op het gebied van beveiliging van computers (hardware en software) maatregelen worden genomen. De mate waarin op die maatregelen moet kunnen worden vertrouwd, wordt bepaald bij het vaststellen van de beveiligingseisen. Bij de accreditatie wordt nagegaan of er voldoende waarborgen zijn om op de beveiligingsmaatregelen te vertrouwen.

SYSTEEMGEBONDEN SPECIFICATIE VAN BEVEILIGINGSEISEN (SSB)

9. Voor alle SYSTEMEN waarin als CONFIDENTIEL UE en hoger gerubriceerde gegevens worden verwerkt, moet een systeemgebonden specificatie van beveiligingseisen (hierna SSB genoemd) worden opgesteld door de operationele instantie van het IT-systeem (OIITS), desgewenst met de inbreng en steun van het projectteam en de INFOSEC-instantie, die wordt goedgekeurd door de IVA. Een SSB is eveneens vereist indien de IVA de beschikbaarheid en integriteit van als RESTREINT UE gerubriceerde of niet-gerubriceerde gegevens gevoelig acht.

10. De SSB wordt zo vroeg mogelijk in de conceptfase van het project geformuleerd, en wordt ontwikkeld en uitgebreid al naargelang het project zich ontwikkelt; de SSB heeft diverse functies op diverse momenten in de looptijd van het project/levensduur van het SYSTEEM.

11. De SSB vormt een bindende overeenkomst tussen de operationele instantie van het IT-systeem en de IVA met het oog op de accreditatie van het SYSTEEM.

12. De SSB is een volledige en uitdrukkelijke verklaring over de beveiligingsprincipes die in acht moeten worden genomen en de gedetailleerde veiligheidseisen waaraan moet worden voldaan. De SSB is gebaseerd op het beveiligingsbeleid en de risicobeoordeling van de Raad, 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 SSB vormt een integrerend bestanddeel van de projectdocumentatie die aan de bevoegde instanties moet worden voorgelegd met het oog op technische, budgettaire en veiligheidsgoedkeuring. In zijn definitieve vorm geeft de SSB uitsluitsel over wat onder een veilig SYSTEEM moet worden verstaan.

BEVEILIGINGSMODI

13. Alle SYSTEMEN waarin als 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";

c) „multi-level".

Hoofdstuk II

Definities

ADDITIONELE MARKERINGEN

14. Zijn een beperkte verspreiding en een bijzondere verwerking nodig (ter aanvulling van die op grond van de rubricering), dan worden additionele markeringen gebruikt, zoals CRYPTO of enige andere door de EU erkende bijzondere aanwijzing over de verwerking.

15. 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.

16. 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 hebben NIET ALLE personen met toegang tot het systeem een gedeelde „need-to-know" 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 beschermd als gold het de categoriebenaming en de hoogste rubriceringsgraad van de verwerkte gegevens tot anders wordt bepaald, en dat tenzij de bestaande markeringsfuncties voldoende betrouwbaar zijn.

17. 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.

18. Onder INFOSEC wordt verstaan: het toepassen van beveiligingsmaatregelen met de bedoeling in communicatie-, informatie- en andere elektronische systemen verwerkte, opgeslagen of doorgezonden gegevens te beschermen tegen al dan niet opzettelijke aantasting van vertrouwelijkheid, 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 opsporingen, documentering van en de beveiliging tegen risico's voor gegevens en SYSTEMEN.

19. 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.

20. Onder PRODUCT VOOR COMPUTERBEVEILIGING wordt verstaan: een generiek beveiligingselement voor computers dat in een IT-systeem wordt geïntegreerd met de bedoeling de vertrouwelijkheid, integriteit of beschikbaarheid van de verwerkte gegevens te versterken of te verzekeren.

21. Onder COMMUNICATIEBEVEILIGING (COMSEC) wordt verstaan: de toepassing van beveiligingsmaatregelen 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.

Opmerking:

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

22. Onder EVALUATIE wordt verstaan: een gedetailleerd technisch onderzoek door een bevoegde instantie van de beveiligingsaspecten van een SYSTEEM of van een product voor versleuteling of computerbeveiliging.

Opmerkingen:

(1) In het kader van een evaluatie wordt onderzocht of de vereiste beveiligingsfunctionaliteit aanwezig is, wordt nagegaan of deze functionaliteit geen schadelijke neveneffecten heeft en wordt de integriteit van de functionaliteit beoordeeld;

(2) In het kader van een evaluatie wordt bepaald in welke mate aan de beveiligingseisen van een SYSTEEM of aan de vooropgestelde 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.

23. Onder CERTIFICATIE wordt verstaan: een formele verklaring, op grond van een onafhankelijke toetsing van de uitvoering en van de resultaten van een evaluatie, over de mate waarin een SYSTEEM voldoet aan de beveiligingseisen, dan wel een product voor computerbeveiliging de vooropgestelde beveiliging kan bieden.

24. 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 voldoende geacht wordt. Accreditatie dient normaliter te gebeuren op basis van de SSB, 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 (OB'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 uitvoering en het onderhoud van de beveiligingsvoorzieningen;

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

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

25. 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 operationele instantie van een IT-systeem worden gecontroleerd;

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

26. BEVEILIGINGSVOORZIENINGEN VAN EEN IT-SYSTEEM bestaan uit alle hardware/firmware/software-functies, -kenmerken en -voorzieningen; operationele procedures, procedures op het gebied van verantwoordelijkheid en toegangscontroles; 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.

27. 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.

28. 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.

29. 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.

30. 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 apart van een IT-zone.

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

Hoofdstuk III

Verantwoordelijkheid voor beveiliging

ALGEMEEN

32. De verantwoordelijkheid van het Beveiligingscomité zoals gedefinieerd in Afdeling 1, punt 4, omvat ook INFOSEC-aangelegenheden. Het Beveiligingscomité organiseert zijn werkzaamheden zodanig dat het deskundig advies over bovengenoemde aangelegenheden kan verstrekken.

33. In geval van beveiligingsproblemen (incidenten, inbreuken, enz.) treden de verantwoordelijke nationale instantie en/of de Dienst beveiliging van het SGR onmiddellijk op. Alle problemen worden gemeld aan de Dienst beveiliging van het SGR.

34. De secretaris-generaal/hoge vertegenwoordiger dan wel, in voorkomend geval, het hoofd van een gedecentraliseerd EU-orgaan, richt een INFOSEC-dienst op die de veiligheidsinstantie adviseert bij de uitvoering en controle van bijzondere beveiligingsvoorzieningen die als onderdeel van SYSTEMEN zijn uitgewerkt.

INSTANTIE VOOR VEILIGHEIDSACCREDITATIE (IVA)

35. De IVA is:

— een NVI;

— een door de secretaris-generaal/hoge vertegenwoordiger aangewezen instantie;

— de veiligheidsinstantie van een gedecentraliseerd EU-orgaan; of

— hun gedetacheerde/aangewezen vertegenwoordigers, al naargelang het systeem dat dient te worden geaccrediteerd.

36. Het is de taak van de IVA, ervoor te zorgen dat SYSTEMEN in overeenstemming zijn met het beveiligingsbeleid van de Raad. Een van haar taken bestaat erin, een SYSTEEM goedkeuring te verlenen om gerubriceerde EU-gegevens te verwerken in zijn operationele omgeving, afhankelijk van het vastgestelde rubriceringsniveau. Wat het SGR en, in voorkomend geval, gedecentraliseerde EU-organen betreft, is de IVA namens de secretaris-generaal/hoge vertegenwoordiger dan wel het hoofd van het gedecentraliseerde orgaan verantwoordelijk voor de beveiliging.

De bevoegdheid van de IVA van het SGR omvat alle in de gebouwen van het SGR functionerende SYSTEMEN. In een lidstaat functionerende SYSTEMEN en bestanddelen van SYSTEMEN blijven onder de bevoegdheid van die lidstaat ressorteren. Indien verschillende bestanddelen van een SYSTEEM onder de bevoegdheid van de IVA van het SGR en andere IVA's komen te vallen, wijzen alle partijen een gemeenschappelijk accreditatieorgaan aan, dat door de IVA van het SGR wordt gecoördineerd.

INFOSEC-INSTANTIE (II)

37. De INFOSEC-instantie is verantwoordelijk voor de werkzaamheden van de INFOSEC-dienst. Wat het SGR en, in voorkomend geval, gedecentraliseerde organen van de EU betreft, houdt de verantwoordelijkheid van de INFOSEC-instantie het volgende in:

— technisch advies en technische bijstand verlenen aan de IVA;

— de ontwikkeling van de SSB ondersteunen;

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

— zo nodig, deelnemen aan accreditatiecommissies/-organen en accreditatie-aanbevelingen op het stuk van INFOSEC doen aan de IVA;

— INFOSEC-opleiding en -scholing ondersteunen;

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

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

OPERATIONELE INSTANTIE VAN HET IT-SYSTEEM (OIITS)

38. De INFOSEC-instantie delegeert de verantwoordelijkheid voor de implementatie en uitvoering van controles en bijzondere beveiligingsvoorzieningen van het SYSTEEM zo snel mogelijk aan de operationele instantie van de OIITS. Deze verantwoordelijkheid geldt voor de volledige levenscyclus van het SYSTEEM, van de projectconceptfase tot de uiteindelijke verwijdering.

39. De OIITS is verantwoordelijk voor alle beveiligingsmaatregelen die als onderdeel van het algemene SYSTEEM zijn uitgewerkt. Deze verantwoordelijkheid omvat ook het opstellen van operationele beveiligingsprocedures (OB's). De OIITS specificeert de beveiligingsnormen en -praktijken waaraan de leverancier van het SYSTEEM moet voldoen.

40. De OIITS kan in voorkomend geval een deel van haar verantwoordelijkheden delegeren, bijvoorbeeld aan de INFOSEC-beveiligingsfunctionaris en de INFOSEC-locatiebeveiligingsfunctionaris.

GEBRUIKERS

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

INFOSEC-OPLEIDING

42. Op verschillende niveaus en voor verschillende personeelscategorieën wordt voorzien in opleiding en scholing op INFOSEC-gebied, al naargelang het geval in het SGR, de gedecentraliseerde EU-organen of het departement van een regering van een lidstaat.

Hoofdstuk IV

Niet-technische beveiligingsmaatregelen

PERSONEELSGERELATEERDE BEVEILIGING

43. Al naargelang 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 Raadsprocedures wordt afgegeven.

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

45. Het specificeren en ontwerpen van SYSTEMEN gebeurt zodanig dat gemakkelijker taken en verantwoordelijkheden aan het personeel kunnen worden toegewezen; het doel daarvan is te voorkomen dat één persoon volledig kennis heeft van c.q. controle heeft over de cruciale punten van de systeembeveiliging, en dat daarentegen twee of meer personen nodig zijn om het systeem of het netwerk te kunnen aanpassen dan wel opzettelijk schade te berokkenen.

FYSIEKE BEVEILIGING

46. IT-zones en afzonderlijke zones met terminals/werkstations (zoals omschreven in de punten 29 en 30) waar als EU CONFIDENTIEL 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 klasse I of II, of, in voorkomend geval, het nationaal equivalent daarvan.

47. 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.

CONTROLE OP DE TOEGANG TOT EEN SYSTEEM

48. 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.

49. Indien gegevens en het materiaal voor toegangscontrole niet langer voor dat doel worden gebruikt, worden zij vernietigd overeenkomstig de punten 61 tot en met 63.

Hoofdstuk V

Technische beveiligingsmaatregelen

GEGEVENSBEVEILIGING

50. 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.

51. Een organisatie en de houders van haar gegevens hebben de 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.

52. 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.

53. 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.

54. 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.

55. 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 goedgekeurde procedure van het SGR of een nationale procedure vernietigd zijn (zie de punten 61 tot en met 63).

CONTROLE VAN EN VERANTWOORDELIJKHEID VOOR GEGEVENS

56. De toegang tot als 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.

57. 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 gemarkeerd en afdoende wordt gecontroleerd.

58. 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 IVA goed te keuren procedures voor de controle van die afzonderlijke outputs vastgesteld. Voor de rubricering SECRET UE en hoger omvatten zulke procedures specifieke instructies met betrekking tot de verantwoordelijkheid voor de gegevens.

BEHANDELING EN CONTROLE VAN VERWIJDERBARE DIGITALE OPSLAGMEDIA

59. Als 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.

60. 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.

DERUBRICERING EN VERNIETIGING VAN DIGITALE OPSLAGMEDIA

61. Digitale opslagmedia die worden gebruikt om gerubriceerde EU-gegevens vast te leggen, kunnen een lagere rubricering krijgen c.q. gederubriceerd worden mits goedgekeurde procedures van het SGR of nationale procedures worden toegepast.

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

63. Is het niet mogelijk digitale opslagmedia een lagere rubricering te geven of opnieuw te gebruiken, dan worden deze conform een goedgekeurde procedure van het SGR of een nationale procedure vernietigd.

COMMUNICATIEBEVEILIGING

64. Indien gerubriceerde EU-gegevens elektromagnetisch worden overgedragen, worden bijzondere maatregelen toegepast om de vertrouwelijkheid, de integriteit en de beschikbaarheid van die overdracht te beschermen. De IVA 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 vertrouwelijkheid, integriteit en beschikbaarheid.

65. Is versleuteling vereist om de vertrouwelijkheid, integriteit en beschikbaarheid te beschermen, dan worden bedoelde methodes of aanverwante producten daartoe specifiek goedgekeurd door de IVA.

66. Tijdens de overdracht wordt de vertrouwelijkheid van als SECRET UE en hoger gerubriceerde gegevens beschermd door middel van methoden of producten voor versleuteling die door de Raad op voorstel van zijn Beveiligingscomité zijn goedgekeurd. Tijdens de overdracht wordt de vertrouwelijkheid van als CONFIDENTIEL UE of RESTREINT UE gerubriceerde gegevens beschermd door methoden of producten voor versleuteling die hetzij door de SG/HR op voorstel van het Beveiligingscomité van de Raad, hetzij door een lidstaat zijn goedgekeurd.

67. Gedetailleerde regels voor de overdracht van gerubriceerde EU-gegevens worden vastgelegd in specifieke beveiligingsinstructies, die door de Raad op voorstel van zijn Beveiligingscomité worden goedgekeurd.

68. In uitzonderlijke operationele omstandigheden kunnen als RESTREINT UE, CONFIDENTIEL UE en SECRET UE gerubriceerde gegevens in niet-versleutelde vorm worden overgedragen, mits daartoe steeds uitdrukkelijk toestemming wordt verleend. Zulke uitzonderlijke omstandigheden doen zich voor

   a) in geval van dreigende of uitgebroken crises, conflicten of oorlogssituaties; alsmede

   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.

69. 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 IVA goedgekeurde software.

INSTALLATIE- EN STRALINGSBEVEILIGING

70. 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.

71. Alle apparatuur wordt in overeenstemming met het huidige beveiligingsbeleid van de Raad geïnstalleerd.

72. SYSTEMEN waarin als 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".

73. Anti-TEMPEST-maatregelen voor installaties van het SGR en gedecentraliseerde EU-organen worden getoetst en goedgekeurd door een TEMPEST-instantie, die wordt aangewezen door de veiligheidsinstantie van het SGR. Wat betreft nationale installaties waarin gerubriceerde EU-gegevens worden verwerkt, is de goedkeurende instantie de erkende nationale instantie die de TEMPEST-goedkeuring verleent.

Hoofdstuk VI

Beveiliging tijdens verwerking

OPERATIONELE BEVEILIGINGSPROCEDURES

74. De operationele beveiligingsprocedures (OB's) definiëren de aan te nemen beveiligingsprincipes, de te volgen operationele procedures en de personele verantwoordelijkheden. De OB's worden opgesteld onder de verantwoordelijkheid van de operationele instantie van het IT-systeem.

BESCHERMING VAN SOFTWARE/CONFIGURATIEBEHEER

75. 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.

76. Nieuwe of gewijzigde softwareversies mogen pas worden gebruikt om gerubriceerde EU-gegevens te verwerken nadat zij door de operationele instantie van het IT-systeem zijn geverifieerd.

CONTROLE OP DE AANWEZIGHEID VAN KWAADAARDIGE SOFTWARE/COMPUTERVIRUSSEN

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

78. Alle digitale opslagmedia die in het SGR of in gedecentraliseerde EU-organen dan wel in de lidstaten worden binnengebracht, dienen te worden gecontroleerd op de aanwezigheid van kwaadaardige software of computervirussen alvorens deze in een SYSTEEM worden geïntegreerd.

ONDERHOUD

79. De contracten en procedures in verband met regulier en ad hoc onderhoud en van SYSTEMEN waarvoor een SSB is voorgelegd, bevatten eisen en afspraken met betrekking tot het onderhoudspersoneel dat een IT-zone betreedt, en de apparatuur die het bij zich heeft.

80. De eisen en de procedures worden duidelijk geformuleerd in respectievelijk de SSB en de OB'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 IVA daarvoor haar goedkeuring verleent.

Hoofdstuk VII

Aanschaffing

81. 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 aanschaffing worden beoordeeld en gecertificeerd door een bevoegde beoordelings- of certificerende instantie, op grond van internationaal erkende criteria (zoals de Common Criteria for Information Technology Security Evaluation, ISO 15408).

82. Bij de keuze voor de huur dan wel 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 IVA, alsmede dat een dergelijke derubricering niet altijd zal kunnen worden goedgekeurd.

ACCREDITATIE

83. Alle SYSTEMEN waarvoor een SSB dient te worden voorgelegd alvorens daarin gerubriceerde EU-gegevens kunnen worden verwerkt, worden door de IVA geaccrediteerd op basis van de informatie die is vervat in de SSB, de operationele beveiligingsprocedures (OB'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 het SGR en de bevoegde veiligheidsinstanties onderling afspraken met betrekking tot de accreditatie.

84. De accreditatie kan worden uitgevoerd overeenkomstig een door de IVA bepaalde accreditatiestrategie die afgestemd is op het SYSTEEM in kwestie.

BEOORDELING EN CERTIFICATIE

85. 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.

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

87. De beoordeling en certificatie worden uitgevoerd overeenkomstig goedgekeurde richtsnoeren door technisch gekwalificeerd en dienovereenkomstig gemachtigd personeel, namens de operationele instantie van het IT-systeem.

88. 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.

89. 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.

ROUTINECONTROLE VAN BEVEILIGINGSVOORZIENINGEN MET HET OOG OP VERLENGING VAN DE ACCREDITATIE

90. De operationele instantie van het IT-systeem legt procedures voor routinecontroles vast, die tot doel hebben na te gaan of alle beveiligingsvoorzieningen van het SYSTEEM nog steeds geldig zijn.

91. In de SSB wordt duidelijk opgesomd en verklaard welke soorten wijzigingen aanleiding geven tot heraccreditatie of vooraf door de IVA 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 operationele instantie zich ervan dat wordt gecontroleerd of de beveiligingsvoorzieningen correct functioneren. Normaliter wordt de accreditatie van het SYSTEEM alleen verlengd indien het resultaat van de controles bevredigend is.

92. Alle SYSTEMEN met beveiligingsvoorzieningen worden regelmatig gecontroleerd of getoetst door de IVA. Wat SYSTEMEN betreft waarin als TRÈS SECRET UE/EU TOP SECRET gerubriceerde gegevens of gegevens met additionele markeringen worden verwerkt, worden de controles op zijn minst jaarlijks uitgevoerd.

Hoofdstuk VIII

Tijdelijk of accidenteel gebruik

BEVEILIGING VAN MICROCOMPUTERS/PERSONAL COMPUTERS

93. Microcomputers/personal computers (PC's) met vaste schijven (of andere permanente opslagmedia) die als standalone 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.

94. 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).

OFFICIEEL GEBRUIK IN DE RAAD VAN PARTICULIERE IT-APPARATUUR

95. 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.

96. Particuliere hardware, software en media mogen alleen met toestemming van het hoofd van de Dienst beveiliging van het SGR een departement van een lidstaat, of een gedecentraliseerd EU-orgaan worden binnengebracht in een zone van klasse I of klasse II waar gerubriceerde EU-gegevens worden verwerkt.

GEBRUIK VAN OFFICIËLE RAADSWERKZAAMHEDEN VAN IT-APPARATUUR DIE IN HET BEZIT IS VAN EEN CONTRACTANT DAN WEL OP NATIONALE BASIS TER BESCHIKKING IS GESTELD

97. Het gebruik van IT-apparatuur die in het bezit is van een contractant en van software in organisaties ter ondersteuning van officiële Raadswerkzaamheden kan worden toegestaan door het hoofd van de Dienst beveiliging van het SGR, een departement van een lidstaat of een gedecentraliseerd EU-orgaan. Het gebruik van op nationale basis ter beschikking gestelde IT-apparatuur en software door ambtenaren in het SGR of in een gedecentraliseerd EU-orgaan kan eveneens worden toegestaan; in dat geval staat de IT-apparatuur onder controle van de desbetreffende inventaris van het SGR. Indien de IT-apparatuur bestemd is om gerubriceerde EU-gegevens te verwerken, moet de bevoegde IVA 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.

AFDELING XII

VRIJGAVE VAN GERUBRICEERDE EU-GEGEVENS AAN DERDE STATEN OF INTERNATIONALE ORGANISATIES

BEGINSELEN VOOR DE VRIJGAVE VAN GERUBRICEERDE EU-GEGEVENS

1. Over de vrijgave van gerubriceerde EU-gegevens aan derde staten of internationale organisaties wordt door de Raad beslist op basis van:

   — soort en inhoud van gegevens;

   — de noodzaak voor de ontvangers om kennis te nemen van de gegevens;

   — de baat die de EU bij vrijgave heeft.

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

2. 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 beveiligingsvoorschriften; het Beveiligingscomité van de Raad dient de Raad in dezen van technisch advies.

3. 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 Raad vereiste bescherming zullen bieden.

GRADEN

4. Wanneer de Raad 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 beveiliging die de bewuste staat of organisatie toepast.

5. Er zijn drie graden van samenwerking:

   Graad 1

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

   Graad 2

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

   Graad 3

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

6. De graad van samenwerking is bepalend voor de beveiligingsvoorschriften — welke in individuele gevallen in het licht van het technisch advies van het Beveiligingscomité van de Raad opnieuw kunnen worden geformuleerd — die de begunstigden verzocht wordt toe te passen ter bescherming van de aan hen vrijgegeven gerubriceerde gegevens. Deze beveiligingsprocedures en -voorschriften worden in detail beschreven in de aanhangsels 4, 5 en 6.

OVEREENKOMSTEN

7. Wanneer de Raad besloten heeft dat er permanent of langdurig behoefte is aan de uitwisseling van gerubriceerde gegevens tussen de EU 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.

8. In geval van incidentele 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 RESTREINT UE.

9. Ontwerp-overeenkomsten inzake beveiligingsprocedures of memoranda van overeenstemming worden door het Beveiligingscomité goedgekeurd voordat zij ter aanneming aan de Raad worden voorgelegd.

10. De nationale veiligheidsinstanties verschaffen de secretaris-generaal/hoge vertegenwoordiger alle nodige 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.

Aanhangsel 1

Lijst van nationale veiligheidsinstanties

BELGIË

Ministerie van Buitenlandse Zaken, Buitenlandse Handel en Outwikkelingssamenwerking
Directie veiligheid — A 01
Karmelietenstraat 15
B-1000 Brussel
Telefoon: 32-2-501 85 14
Fax: 32-2-501 80 58
Telex: 21376
Telegraaf: Directie veiligheid A01 — MINAFET

DENEMARKEN

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefoon: 45 33 14 88 88
Fax: 45 38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø.
Telefoon: 45 33 32 55 66
Fax: 45 33 93 13 20

DUITSLAND

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefoon: 49-30-39 81 15 28
Fax: 49-30-39 81 16 10

GRIEKENLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετράωρο)
Φαξ: 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos — Athens
Greece
Telefoon: 00 30-1-655 22 03 (kantooruren)
00 30-1-655 22 05 (24 uur)
Fax: 00 30-1-642 69 40

SPANJE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
Telefoon: 34-91-372 57 07
Fax: 34-91-372 58 08
E-mail: nsa-sp@areatec.com

FRANKRIJK

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefoon: 33-0-144 18 81 80
Fax: 33-0-144 18 82 00
Telex: SEGEDEFNAT 200019
Telegraaf: SEGEDEFNAT PARIS

IERLAND

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefoon: 353-1-478 08 22
Fax: 353-1-478 14 84

ITALIË

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefoon: 39-06-627 47 75
Fax: 39-06-614 33 97
Telex: 623876 AQUILA 1
Telegraaf: ess: PCM-ANS-UCSI-ROMA

LUXEMBURG

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L-1023 Luxembourg
Telefoon: 352-478 22 10 central
352-478 22 35 direct
Fax: 352-478 22 43
352-478 22 71
Telex: 3481 SERET LU
Telegraaf: MIN D'ETAT — ANS

NEDERLAND

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefoon: 31-70-320 44 00
Fax: 31-70-320 07 33
Telex: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Telefoon: 31-70-318 70 60
Fax: 31-70-318 79 51

OOSTENRIJK

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefoon: 43-1-531 15 34 64
Fax: 43-1-531 8 52 19

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefoon: 351-21-301 55 10
351-21-301 00 01, toestel 20 45 37
Fax: 351-21-302 03 50

FINLAND

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefoon: 358-9-13 41 53 38
Fax: 358-9-13 41 53 03

ZWEDEN

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefoon: 46-8-405 54 44
Fax: 46-8-723 11 76

VERENIGD KONINKRIJK

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1 AH
Telefoon: 44-20-72 70 87 51
Fax: 44-20-76 30 14 28
Telegraaf: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Aanhangsel 2

Vergelijking van de nationale beveiligingsrubriceringen

EU-rubricering	Trés Secret UE/EU TOP Secret	EU Secret	EU Confidentiel	EU Restricted
NAVO-rubricering ([1])				
WEU-rubricering	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Duitsland	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Oostenrijk	Streng geheim	Geheim	Vertraulich	Eingeschränkt
België	Très Secret Zeer geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Denemarken	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Spanje	Secreto	Reservado	Confidencial	Difusion Limitada
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Frankrijk	Très Secret Défense ([3])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Griekenland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Ierland	Top Secret	Secret	Confidential	Restricted
Italië	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Nederland	STG Zeer geheim	STG Geheim	STG Confidentieel	
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Verenigd Koninkrijk	Top Secret	Secret	Confidential	Restricted
Zweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

([1]) NAVO: de correspondentie met de NAVO-rubriceringsgraden wordt vastgesteld bij de onderhandelingen over de beveiligingsovereenkomst tussen de Europese Unie en de NAVO.
([2]) Duitsland: VS = Verschlußsache (versleutelde informatie)
([3]) Frankrijk: met „Très Secret Défense“ gemerkte documenten, die betrekking hebben op regeringsprioriteiten, kunnen alleen worden uitgewisseld met toestemming van de eerste minister.

Aanhangsel 3

Praktische rubriceringsgids

Deze gids is indicatief en mag niet geïnterpreteerd worden als wijziging van de inhoudelijke bepalingen van de afdelingen II en III.

Rubricering	wanneer	wie	markeringen	lagere rubricering /derubricering/vernietiging	
				wie	wanneer
TRÈS 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 een of meer van haar lidstaten [II.1]	Indien het compromitteren van als TRÈS 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	Lidstaten: naar behoren gemachtigde personen (opstellers) [III.4]; SGR: naar behoren gemachtigde personen (opstellers) [III.4], SG/HV en PlvSG Opstellers vermelden 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 [III.10]	De rubricering TRÈS SECRET UE/EU TOP SECRET wordt toegepast op TRÈS SECRET UE/EU TOP SECRET-documenten; waar van toepassing wordt de defensiemarkering ESDP/PESD mechanisch en handmatig aangebracht [II.8] De EU-rubriceringen en -markeringen worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum. 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. [VII.1]	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, de SG/HV of de PlvSG, welke de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte brengen. [III.9] TRÈS SECRET UE/EU TOP SECRET-documenten mogen alleen vernietigd worden door het centrale of subregister register dat voor die documenten verantwoordelijk is. Elk vernietigd document wordt genoteerd in een proces-verbaal van vernietiging dat ondertekend wordt door de TRÈS SECRET UE/EU TOP SECRET-controlefunctionaris en de functionaris die getuige is bij de vernietiging en voor de TRÈS SECRET UE/EU TOP SECRET-graad gemachtigd is. Hiervan wordt aantekening gemaakt in het logboek. Het register moet de processenverbaal van vernietiging samen met de verspreidingsformulieren gedurende tien jaar bewaren. [VII.31]	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd. [VII.31] TRÈS SECRET UE/EU TOP SECRET-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van TRÈS SECRET UE/EU TOP SECRET-documenten, zoals kladversies, ontwerpteksten, getypte aantekeningen en carbonpapier, worden onder toezicht van een TRÈS SECRET UE/EU TOP SECRET-functionaris vernietigd door verbranding, verpulping, versnippering of een andere methode waardoor de documenten onherkenbaar en onherstelbaar vernietigd worden. [VII.31]

Rubricering	wanneer	wie	markeringen	lagere rubricering /derubricering/vernietiging	
				wie	wanneer
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 een of meer van haar lidstaten [II.2]	Indien het compromitteren van als 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	Lidstaten: naar behoren gemachtigde personen (opstellers) [III.2]; SGR en gedecentraliseerde EU-organen: naar behoren gemachtigde personen (opstellers) [III.2], directeuren-generaal, SG/HV en PlvSG Opstellers vermelden 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 [III.10]	De rubricering SECRET UE wordt toegepast op SECRET UE-documenten; waar van toepassing wordt de defensiemarkering ESDP/PESD mechanisch en handmatig aangebracht [II.8] De EU-rubriceringen en -markeringen worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum. 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. [VII.1]	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, de SG/HV of de PlvSG, welke de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte brengen. [III.9] 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 SECRET UE-documenten worden genoteerd in een ondertekend proces-verbaal van vernietiging, dat door het register, met de verspreidingsformulieren, gedurende ten minste drie jaar bewaard wordt. [VII.32]	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd. [VII.31] SECRET UE-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van SECRET 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. [VII.31&32]

Rubricering	wanneer	wie	markeringen	lagere rubricering /derubricering/vernietiging	
				wie	wanneer
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 een of meer van haar lidstaten [II.3]	Indien het compromitteren van als CONFIDENTIEL UE gerubriceerd materiaal: — de diplomatieke betrekkingen materiële schade zou kunnen berokkenen, dat wil zeggen zou kunnen leiden tot officieel protest of andere sancties — 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	Lidstaten: naar behoren gemachtigde personen (opstellers) [III.2]; SGR en gedecentraliseerde EU-organen: naar behoren gemachtigde personen (opstellers) [III.2], directeuren-generaal, SG/HV en PlvSG Opstellers vermelden 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 [III.10]	De rubricering CONFIDENTIEL UE wordt toegepast op CONFIDENTIEL UE-documenten; waar van toepassing wordt de defensiemarkering ESDP/PESD mechanisch en handmatig aangebracht, of door het drukken op voorgemerkt, geregistreerd papier [II.8] De EU-rubriceringen en -markeringen worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum. 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. [VII.1]	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, de SG/HV of de PlvSG, welke de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte brengen. [III.9] 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 het SGR of gedecentraliseerde EU-organen, volgens de instructies van de SG-HV of PlvSG. [VII.33]	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd. [VII.31] CONFIDENTIEL UE-documenten, alsmede alle gerubriceerde afvalproducten van het vervaardigen van 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. [VII.31&33]

Rubricering	wanneer	wie	markeringen	lagere rubricering /derubricering/vernietiging	
				wie	wanneer
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 een of meer van haar lidstaten [II.4]	Indien het compromitteren van als RESTREINT UE gerubriceerd materiaal: — nadelig 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	Lidstaten: naar behoren gemachtigde personen (opstellers) [III.2]; SGR en gedecentraliseerde EU-organen: naar behoren gemachtigde personen (opstellers) [III.2], directeuren-generaal, SG/HV en PlvSG Opstellers vermelden 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 [III.10]	De rubricering RESTREINT UE wordt toegepast op RESTREINT UE-documenten; waar van toepassing wordt de defensiemarkering ESDP/PESD met mechanische of elektronische middelen aangebracht [II.8] De EU-rubriceringen en -markeringen worden midden bovenaan en midden onderaan elke bladzijde vermeld; elke bladzijde wordt genummerd. Elk document krijgt een referentienummer en een datum. [VII.1]	Derubricering of lagere rubricering is de uitsluitende verantwoordelijkheid van de opsteller, de SG/HV of de PlvSG, welke de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte brengen. [III.9] RESTREINT UE-documenten worden vernietigd door het register dat voor die documenten verantwoordelijk is overeenkomstig de nationale voorschriften of, in het geval van het SGR of gedecentraliseerde EU-organen, volgens de instructies van de SG/HV of PlvSG [VII.34]	Overtollige kopieën en overbodig geworden documenten moeten worden vernietigd. [VII.31]

Aanhangsel 4

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 Raad.

2. De Raad kan de bevoegdheid om te besluiten gerubriceerde gegevens vrij te geven delegeren. In de bevoegdheidsoverdracht worden de aard van de vrij te geven gegevens en hun rubriceringsgraad, die normaliter niet hoger is dan CONFIDENTIEL UE, vermeld.

3. Onder voorbehoud van de sluiting van een beveiligingsovereenkomst worden verzoeken om vrijgave van gerubriceerde EU-gegevens aan de secretaris-generaal/hoge vertegenwoordiger gericht door de beveiligingsinstanties van de betrokken staten of internationale organisaties, waarbij deze verklaren waarvoor de vrijgave bedoeld is en van welke aard de gerubriceerde gegevens zijn waarvan zij vrijgave wensen.

   Verzoeken kunnen ook worden gedaan door lidstaten of gedecentraliseerde EU-organen die de vrijgave van gerubriceerde EU-gegevens wenselijk achten; daarbij geven zij aan wat het doel is van de vrijgave en welke baten de EU erbij heeft, en specificeren zij de aard en de rubricering van de gegevens waarvan zij vrijgave wensen.

4. Het verzoek wordt in overweging genomen door het SGR dat

   — advies inwint bij de lidstaat of, indien passend, het gedecentraliseerd EU-orgaan waarvan de vrij te geven gegevens afkomstig zijn;

   — de nodige contacten legt 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 de beveiligingsvoorschriften van de Raad zullen worden beschermd;

   — technisch advies inwint bij de nationale veiligheidsinstanties van de lidstaten met betrekking tot het vertrouwen dat kan worden gesteld in de begunstigde staten of internationale organen.

5. Het SGR legt het verzoek en de aanbeveling van de Dienst beveiliging voor aan de Raad opdat deze er een besluit over neemt.

BEVEILIGINGSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

6. De secretaris-generaal/hoge vertegenwoordiger stelt de begunstigde staten of internationale organisaties in kennis van het besluit van de Raad houdende toestemming tot vrijgave van gerubriceerde EU-gegevens, en zendt deze zoveel kopieën van de beveiligingsvoorschriften van de Raad als nodig geacht wordt. Indien het verzoek is ingediend door een lidstaat stelt deze de begunstigde in kennis van de toestemming tot vrijgave hiervan. 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 beveiligingsvoorschriften van de Raad en meer bepaald de volgende 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 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 op basis van de bepalingen van afdeling VII van de beveiligingsvoorschriften van de Raad. Hierin wordt met name gespecificeerd aan welke registers de gerubriceerde EU-gegevens worden toegestuurd.

b) Indien de gerubriceerde gegevens waarvan de Raad de vrijgave heeft goedgekeurd EU TOP SECRET-gegevens bevatten, zet de begunstigde staat of internationale organisatie een centraal EU-register en zo nodig EU-subregisters op. Deze registers vallen onder de bepalingen van afdeling VIII van de beveiligingsvoorschriften van de Raad.

9. *Registratie*

Zodra een register een als 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 VI van de beveiligingsvoorschriften van de Raad. Kopieën van het proces-verbaal van vernietiging voor SECRET UE- en TRÈS 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 CONFIDENTIEL UE of 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 TRÈS 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 de Dienst beveiliging van het SGR.

13. *Inbreuken op de beveiligingsvoorschriften*

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 de Dienst beveiliging van het SGR, 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 de Dienst beveiliging van het SGR aanbevolen maatregelen om herhaling te voorkomen, uitvoeren.

14. *Inspecties*

De Dienst beveiliging van het SGR 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 de beveiligingsvoorschriften van de Raad zijn nageleefd.

Aanhangsel 5

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 Raad. In beginsel is de bevoegdheid beperkt tot gegevens met een rubricering tot en met SECRET UE; nationale gegevens die specifiek voorbehouden zijn aan de lidstaten en categorieën gerubriceerde EU-gegevens die met speciale markeringen beschermd zijn, zijn hiervan uitgesloten.

2. De Raad kan het besluit om gerubriceerde gegevens vrij te geven delegeren. In de bevoegdheidsoverdracht worden de in punt 1 omschreven beperkingen, de aard van de vrij te geven gegevens en hun rubriceringsgraad, die niet hoger is dan RESTREINT UE, vermeld.

3. Onder voorbehoud van de sluiting van een beveiligingsovereenkomst worden verzoeken om vrijgave van gerubriceerde EU-gegevens aan de secretaris-generaal/hoge vertegenwoordiger gericht door de beveiligingsinstanties van de betrokken staten of internationale organisaties, waarbij deze aangeven wat het doel is van de vrijgave en de aard en de rubricering van de gegevens waarvan zij vrijgave wensen.

   Verzoeken kunnen ook worden gedaan door lidstaten of gedecentraliseerde EU-organen die de vrijgave van gerubriceerde gegevens wenselijk achten; daarbij geven zij aan wat het doel is van de vrijgave en welke baten de EU erbij heeft, en specificeren zij de aard en de rubricering van de gegevens waarvan zij vrijgave wensen.

4. Het verzoek wordt in overweging genomen door het SGR dat:

   — advies inwint bij de lidstaat of indien passend het gedecentraliseerd EU-orgaan waarvan de vrij te geven gegevens afkomstig zijn;

   — eerste contacten legt 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;

   — een bijeenkomst belegt van het Beveiligingscomité van de Raad of zo nodig, volgens een stilzwijgende procedure, navraag doet bij de nationale veiligheidsinstanties van de lidstaten om het technisch advies van het Beveiligingscomité in te winnen.

5. Het technisch advies van het Beveiligingscomité van de Raad 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 vermelden of verwijderen van EU-rubriceringsopschriften, specifieke markeringen enz.);

   — lagere rubricering of derubricering door de instantie waarvan de gegevens afkomstig zijn voordat deze worden vrijgegeven aan de begunstigde landen of internationale organisaties ([1]).

([1]) Dit impliceert dat deze instantie de in afdeling III, punt 9, omschreven procedure toepast op alle kopieën die binnen de EU worden verspreid.

6. De secretaris-generaal/hoge vertegenwoordiger legt het verzoek en de door de Dienst Beveiliging van het SGR bij het Beveiligingscomité van de Raad ingewonnen technisch advies voor aan de Raad opdat deze er een besluit over neemt.

BEVEILIGINGSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

7. Het besluit van de Raad houdende toestemming tot vrijgave van gerubriceerde EU-gegevens wordt door de secretaris-generaal/hoge vertegenwoordiger samen met een vergelijkende tabel van de in de EU en de betrokken staten of organisaties van toepassing zijnde rubriceringen ter kennis gebracht van de begunstigde staten of internationale organisaties. Indien het verzoek is ingediend door een lidstaat stelt deze de begunstigden van de toestemming tot vrijgave hiervan in kennis.

   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 beveiligingsvoorschriften van de Raad.

8. De volgende beschermingsvoorschriften worden vastgesteld, tenzij de Raad, na inwinning van het technisch advies van het Beveiligingscomité van de Raad, besluit een bijzondere procedure vast te stellen voor de verwerking van gerubriceerde EU-documenten (niet vermelden van de EU-rubricering, specifieke markering enz.).

   In dat geval worden de regels aangepast.

9. *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 EU vrijgegeven gerubriceerde gegevens zijn in het bezit van een nationale veiligheidsmachtiging of toegangsmachtiging, ingeval van nationale gerubriceerde gegevens, 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 de secretaris-generaal/hoge vertegenwoordiger gestuurd.

10. *Overdracht van documenten*

   a) De praktische procedures voor de overdracht van documenten worden geregeld tussen de Dienst Beveiliging van het SGR en de beveiligingsinstanties van de ontvangende staten of internationale organisaties, dit op basis van de in Afdeling VII van deze voorschriften uiteengezette regels. Hierin zullen in het bijzonder de exacte adressen worden gespecificeerd waarnaar de documenten moeten worden gestuurd alsmede de koerier- of postdiensten die gebruikt worden voor de overdracht van gerubriceerde EU-gegevens.

   b) Als CONFIDENTIEL UE en hoger gerubriceerde documenten worden in een dubbele enveloppe doorgegeven. Op de binnenenveloppe wordt „EU" en de beveiligingsrubricering aangebracht. 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.

11. *Registratie bij ontvangst*

   De nationale veiligheidsinstantie van de geadresseerde staat of haar tegenhanger in de staat die namens de regering de door de EU 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.

12. *Terugsturen van documenten*

Wanneer de ontvanger een gerubriceerd document terugstuurt naar de Raad of de lidstaat die het heeft vrijgegeven, handelt deze in overeenstemming met punt 10.

13. *Bescherming*

a) Wanneer de documenten niet gebruikt worden, 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) 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 de Dienst Beveiliging van het SGR mogen er geen fotokopieën of uittreksels worden gemaakt van als CONFIDENTIEL UE of hoger gerubriceerde documenten.

d) De procedure voor snelle en volledige vernietiging van documenten in noodgevallen wordt vastgesteld en bevestigd door de Dienst Beveiliging van het SGR.

14. *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.

15. *Inbreuken op de beveiligingsvoorschriften*

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 de Dienst Beveiliging van het SGR 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 de Dienst Beveiliging van het SGR);

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.

16. *Inspecties*

De Dienst beveiliging van het SGR 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.

17. *Rapportage*

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

Aanhangsel 6

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

Derdegraadssamenwerking

PROCEDURES

1. In bepaalde gevallen kan de Raad het wenselijk achten om onder bepaalde speciale omstandigheden samen te werken met staten of organisaties die niet de door de beveiligingsvoorschriften van de Raad vereiste garanties kunnen bieden terwijl de gewenste samenwerking wel noopt tot vrijgave van gerubriceerde EU-gegevens. In dat geval worden specifiek aan de lidstaten voorbehouden nationale gegevens uitgesloten van vrijgave.

2. Onder dergelijke speciale omstandigheden worden verzoeken om samenwerking met de EU afkomstig van derde staten of internationale organisaties, of voorgesteld door lidstaten of door gedecentraliseerde EU-organen, in eerste instantie inhoudelijk beoordeeld door de Raad, die zonodig advies inwint bij de lidstaat of het gedecentraliseerd orgaan waarvan de gegevens afkomstig zijn. De Raad 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.

3. Indien de Raad voorstander is van vrijgave, is de secretaris-generaal/hoge vertegenwoordiger verantwoordelijk voor het bijeenroepen van het Beveiligingscomité van de Raad of voor het, zonodig volgens een stilzwijgende procedure, navraag doen bij de nationale veiligheidsinstanties van de lidstaten om het technisch advies van het beveiligingscomité in te winnen.

4. Het technisch advies van het Beveiligingscomité van de Raad behelst:

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

   b) de rubricering van de vrij te geven gegevens, waar passend, met het oog op de aard ervan;

   c) lagere rubricering of derubricering van de gegevens door de instantie waarvan de gegevens afkomstig zijn voordat ze worden vrijgegeven aan de betrokken landen of internationale organisaties [1];

   d) procedures voor de verwerking van de vrij te geven documenten (zie punt 5 hieronder);

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

5. De documenten die worden vrijgegeven aan de in dit aanhangsel bestreken staten of organisaties worden in beginsel verstrekt zonder referentie naar de bron of EU-rubricering. Het Beveiligingscomité van de Raad 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 (zie voorbeelden in punt 14).

6. De Dienst beveiliging van het SGR legt het technisch advies van het Beveiligingscomité aan de Raad voor en voegt daar waar nodig de voorstellen voor de bevoegdheidsoverdrachten aan toe die vereist zijn voor de uitvoering van de taak, vooral in urgente omstandigheden.

7. Zodra de Raad heeft ingestemd met de vrijgave van gerubriceerde EU-gegevens en met de praktische uitvoeringsprocedures legt de Dienst beveiliging van het SGR de nodige contacten met de beveiligingsinstanties van de betrokken staat of organisatie om de toepassing van de beoogde beveiligingsmaatregelen te vergemakkelijken.

---

[1] Dit impliceert dat deze instanties de in afdeling III, punt 9, omschreven procedure toepast op alle kopieën die binnen de EU worden verspreid.

8. Bij wijze van referentie verspreidt de Dienst beveiliging van het SGR onder alle lidstaten en waar passend gedecentraliseerde EU-organen een tabel waarin de aard en de rubricering van de gegevens worden samengevat en de organisaties en landen worden opgesomd waaraan deze gegevens, na besluit van de Raad, kunnen worden vrijgegeven.

9. De nationale veiligheidsinstanties van de lidstaat van vrijgave of de Dienst beveiliging van het SGR neemt de nodige maatregelen om latere schade-evaluaties en herzieningen van de procedures te vergemakkelijken.

10. Indien er zich een wijziging voordoet in de voorwaarden van de samenwerking, wordt de Raad hiervan in kennis gebracht.

BEVEILIGINGSVOORSCHRIFTEN VOOR DE BEGUNSTIGDEN

11. Het besluit van de Raad houdende toestemming tot vrijgave van gerubriceerde EU-gegevens wordt samen met de door het Beveiligingscomité van de Raad voorgestelde en door de Raad goedgekeurde gedetailleerde beschermingsvoorschriften door de secretaris-generaal/hoge vertegenwoordiger ter kennis gebracht van de begunstigde staten of internationale organisaties. Indien het verzoek is ingediend door een lidstaat stelt deze de begunstigden van de toestemming tot vrijgave hiervan in kennis.

    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 Raad goedgekeurde samenwerking;

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

12. *Overdracht van documenten*

    a) De praktische procedures voor de overdracht van documenten worden geregeld tussen de Dienst beveiliging van het SGR 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 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.

13. *Registratie bij ontvangst*

    De nationale veiligheidsinstantie van de geadresseerde staat of haar tegenhanger in de staat die namens de regering de door de EU 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.

14. *Gebruik en bescherming van de uitgewisselde gerubriceerde gegevens*

    a) Als 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 tot naar behoren gemachtigde personen. Als SECRET UE gerubriceerde gegevens worden verzonden per diplomatiek valies, beveiligde postdiensten en beveiligde telecommunicatiekanalen. Een 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 SECRET UE-documenten worden ontvangstbewijzen uitgeschreven.

b) Als 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 CONFIDENTIEL UE gerubriceerde gegevens worden verstuurd per diplomatiek valies, 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 RESTRICTED 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.

15. *Vernietiging*

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

16. *Inbreuken op de beveiligingsvoorschriften*

Wanneer als CONFIDENTIEL UE of 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. Wanneer het resultaat positief is, wordt de instantie waarvan de gegevens afkomstig zijn hiervan in kennis gesteld. Indien het ontoereikende procedures of opslagmethodes zijn die tot de compromittering hebben geleid, worden de nodige stappen gezet om deze te verbeteren. De secretaris-generaal/hoge vertegenwoordiger of de nationale veiligheidsinstantie van de lidstaat die de gecompromitteerde gegevens heeft vrijgegeven, kan de begunstigde verzoeken het onderzoek nader toe te lichten.