►**B**

RÅDETS AFGØRELSE

af 19. marts 2001

om vedtagelse af Rådets sikkerhedsforskrifter

(2001/264/EF)

(EFT L 101 af 11.4.2001, s. 1)

Ændret ved:

		Tidende		
		nr.	side	dato
►**M1**	Rådets afgørelse 2004/194/EF af 10. februar 2004	L 63	48	28.2.2004
►**M2**	Rådets afgørelse 2005/571/EF af 12. juli 2005	L 193	31	23.7.2005

▼B

RÅDETS AFGØRELSE

af 19. marts 2001

om vedtagelse af Rådets sikkerhedsforskrifter

(2001/264/EF)

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 207, stk. 3,

under henvisning til Rådets afgørelse 2000/396/EF, EKSF, Euratom af 5. juni 2000 om vedtagelse af Rådets forretningsorden ([1]), særlig artikel 24 heri, og

ud fra følgende betragtninger:

(1) For at udbygge Rådets virksomhed på områder, som kræver beskyttelse af visse oplysninger, er det hensigtsmæssigt at indføre en overordnet sikkerhedsordning, der omfatter både Rådet, dets Generalsekretariat og medlemsstaterne.

(2) Denne ordning bør i én og samme tekst behandle de spørgsmål, der har været omfattet af alle tidligere afgørelser og bestemmelser på området.

(3) Størstedelen af de EU-oplysninger, der klassificeres CONFIDENTIEL UE eller højere, vil i praksis dreje sig om den fælles sikkerheds- og forsvarspolitik.

(4) For at denne sikkerhedsordning kan blive effektiv, bør medlemsstaterne omfattes af ordningen og træffe de nationale foranstaltninger, der er nødvendige for at overholde bestemmelserne i denne afgørelse i situationer, hvor deres kompetente myndigheder og disses medarbejdere behandler EU-klassificerede oplysninger.

(5) Rådet hilser med tilfredshed, at Kommissionen på den dato, hvorfra denne afgørelse anvendes, ligeledes indfører en samlet ordning, der er i overensstemmelse med bilagene hertil, så det sikres, at Unionens beslutningsproces kan fungere tilfredsstillende.

(6) Rådet understreger, at det er vigtigt, at Europa-Parlamentet og Kommissionen i relevant omfang følger de forskrifter og standarder for sikkerhedsbeskyttelse, der er nødvendige for at beskytte Unionens og dens medlemsstaters interesser.

(7) Denne afgørelse gælder med forbehold af artikel 255 i traktaten og instrumenter til gennemførelse heraf.

(8) Denne afgørelse berører ikke gældende praksis i medlemsstaterne med hensyn til underretning af de nationale parlamenter om Unionens virksomhed —

TRUFFET FØLGENDE AFGØRELSE:

Artikel 1

Rådets sikkerhedsforskrifter, som findes i bilaget, godkendes herved.

Artikel 2

1. Generalsekretæren/den højtstående repræsentant træffer passende foranstaltninger til at sikre, at de i artikel 1 nævnte forskrifter overholdes i Generalsekretariatet for Rådet (i det følgende benævnt »GSR«), af GSR's tjenestemænd og øvrige ansatte, af GSR's eksterne tjenesteleverandører og af personale udstationeret ved GSR samt inden

([1]) EFT L 149 af 23.6.2000, s. 21.

▼B

for såvel Rådets som EU's decentrale organers bygninger og områder i forbindelse med behandling af EU-klassificerede oplysninger ([1]).

2. Medlemsstaterne træffer i overensstemmelse med deres nationale ordninger passende foranstaltninger til at sikre, at de i artikel 1 nævnte bestemmelser overholdes, inden for deres tjenester og deres bygninger, af følgende kategorier af personer i forbindelse med behandling af EU-klassificerede oplysninger:

a) medlemmer af medlemsstaternes faste repræsentationer ved EU samt medlemmer af medlemsstaternes delegationer, der deltager i møder i Rådet eller dets organer eller i andre rådsaktiviteter

b) andre medlemmer af medlemsstaternes administrationer, uanset om de pågældende gør tjeneste på medlemsstaternes område eller i tredjelande, når de behandler EU-klassificerede oplysninger, og

c) medlemsstaternes eksterne tjenesteleverandører og udstationerede medarbejdere, når de behandler EU-klassificerede oplysninger.

Medlemsstaterne underretter straks GSR om de trufne foranstaltninger.

3. De i stk. 1 og 2 nævnte foranstaltninger træffes inden den 30. november 2001.

Artikel 3

I overensstemmelse med de grundlæggende principper og minimumsstandarder for sikkerhed, der er fastsat i bilagets del I, kan generalsekretæren/den højtstående repræsentant træffe foranstaltninger i henhold til bilagets del II, afsnit I, punkt 1 og 2.

Artikel 4

Denne afgørelse træder fra datoen for dens anvendelse i stedet for:

a) Rådets afgørelse nr. 98/319/EF af 27. april 1998 om procedurer, hvorefter tjenestemænd og øvrige ansatte i GSR kan sikkerhedsgodkendes med henblik på at få indsigt i klassificerede oplysninger i Rådets besiddelse ([2])

b) afgørelse truffet af generalsekretæren/den højtstående repræsentant den 27. juli 2000 om de foranstaltninger, der skal anvendes i GSR til beskyttelse af klassificerede oplysninger ([3])

c) afgørelse nr. 433/97 af 22. maj 1997 truffet af generalsekretæren for Rådet om proceduren for sikkerhedsgodkendelse af tjenestemænd, der betjener CORTESY-systemet.

Artikel 5

1. Denne afgørelse træder i kraft på datoen for offentliggørelsen.

2. Den anvendes fra den 1. december 2001.

([1]) Jf. Rådets konklusioner af 10.11.2000.
([2]) EFT L 140 af 12.5.1998, s. 12.
([3]) EFT C 239 af 23.8.2000, s. 1.

▼B

BILAG

SIKKERHEDSFORSKRIFTER FOR RÅDET FOR DEN EUROPÆISKE UNION

▼B

INDHOLDSFORTEGNELSE

▼B

Tillæg 6

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande eller internationale organisationer — Niveau 3 samarbejde…

▼B

DEL I

GRUNDLÆGGENDE PRINCIPPER OG MINIMUMSSTANDARDER FOR SIKKERHEDSBESKYTTELSE

INDLEDNING

1. I disse forskrifter fastlægges de grundlæggende principper og minimumsstandarder for sikkerhedsbeskyttelse og den måde, hvorpå disse skal overholdes ikke blot af Rådet og Generalsekretariatet for Rådet (i det følgende benævnt »GSR«), men også af medlemsstaterne og Den Europæiske Unions decentrale organer (i det følgende benævnt »EU's decentrale organer«) for at værne om sikkerheden og for at sikre, at der gælder en fælles standard for sikkerhedsbeskyttelse.

2. Ved »EU-klassificerede oplysninger« forstås alle oplysninger og ethvert materiale, der i tilfælde af videregivelse uden dertil indhentet bemyndigelse i forskellig grad ville kunne forvolde EU's interesser eller en eller flere af dets medlemsstater skade, uanset om sådanne oplysninger og sådant materiale er udstedt af EU eller modtages fra medlemsstater, tredjelande eller internationale organisationer.

3. I disse forskrifter forstås ved:

   a) »dokument« enhver form for skrivelse, note, referat, rapport, memorandum, signal/meddelelse, skitse, foto, diapositiv, film, kort, diagram, plan, notesbog, stencil, karbonpapir, farvebånd til skrivemaskine eller printer, bånd, kassette, edb-diskette, cd-rom eller andet fysisk medium, hvori eller hvorpå oplysninger er registreret

   b) »materiale« et dokument som defineret i litra a) samt alle former for udstyr eller våben, både færdigfremstillet og under fremstilling.

4. Sikkerhedsbeskyttelsens vigtigste formål er:

   a) at beskytte EU-klassificerede oplysninger mod spionage, lækage eller uautoriseret videregivelse

   b) at beskytte EU-oplysninger, der behandles i kommunikations- og informationssystemer og -netværk, mod risikoen for uautoriseret ændring og for, at de ikke er til rådighed, når de skal anvendes

   c) at beskytte anlæg, der rummer EU-oplysninger, mod sabotage, hærværk og anden forsætlig skade

   d) i tilfælde af brud på sikkerhedsforskrifterne at vurdere den forvoldte skade, begrænse følgerne og træffe de nødvendige foranstaltninger for at undgå gentagelse.

5. Grundlaget for en effektiv sikkerhedsbeskyttelse er:

   a) at der i hver medlemsstat udpeges en national sikkerhedsmyndighed, som er ansvarlig for:

      i) indsamling og registrering af efterretninger om spionage, sabotage, terrorisme og anden undergravende virksomhed, og

      ii) underretning og rådgivning af myndighederne og derigennem af Rådet om sikkerhedsrisici og modforholdsregler

   b) at der både i hver medlemsstat og i GSR udpeges en teknisk INFOSEC-myndighed, som inden for den pågældende sikkerhedsorganisation er ansvarlig for at underrette og rådgive om tekniske sikkerhedsrisici og modforholdsregler

   c) at der er et løbende samarbejde mellem ministerier, offentlige organer og relevante tjenestegrene i GSR med henblik på alt efter omstændighederne at fastslå eller anbefale:

      i) hvilke oplysninger, ressourcer og anlæg det er nødvendigt at beskytte, og

      ii) fælles standarder for sikkerhedsbeskyttelse.

6. Der skal udvises stor omhu og eftertanke ved udvælgelsen af, hvilke oplysninger og hvilket materiale der skal sikkerhedsbeskyttes, og ved vurderingen af, hvilken grad af sikkerhedsbeskyttelse der er behov for. Det er afgørende, at klassifikationsgraden stemmer overens med den sikkerhedsrisiko, som den enkelte oplysning eller det enkelte materiale skal beskyttes mod. For at sikre en smidig informationsstrøm skal der træffes foranstaltninger for at undgå, at der anvendes en for høj klassifikationsgrad. Klassificeringsordningen er det instrument, hvormed disse principper skal gennemføres; der bør anvendes en tilsvarende klassificeringsordning ved

▼B

planlægning og tilrettelæggelse af beskyttelsen mod spionage, sabotage, terrorisme og andre trusler, således at de vigtigste bygninger og områder, der rummer klassificerede oplysninger, og de mest følsomme steder i disse bygninger og områder sikres bedst.

GRUNDLÆGGENDE PRINCIPPER

7. **Sikkerhedsforanstaltningerne skal:**

a) omfatte alle personer med adgang til klassificerede oplysninger, informationsbærende medier med klassificerede oplysninger, alle bygninger og områder, der rummer sådanne oplysninger, og vigtige anlæg

b) tage sigte på at identificere personer, som kunne udgøre en sikkerhedsmæssig risiko for klassificerede oplysninger og vigtige anlæg, der rummer klassificerede oplysninger, og enten forhindre, at de får indsigt heri, eller fjerne dem

c) forhindre, at uautoriserede personer får indsigt i klassificerede oplysninger eller adgang til anlæg, der indeholder sådanne oplysninger

d) sikre, at klassificerede oplysninger kun videregives til de personer, for hvem aktindsigt er tjenstlig nødvendig (»need-to-know«-princippet), hvilket er af afgørende betydning for alle sikkerhedsaspekter

e) sikre alle oplysningers integritet (dvs. hindre forvanskning eller uautoriseret ændring/slettelse uden bemyndigelse) og tilgængelighed (dvs. sikre, at de er til rådighed for autoriserede brugere, når de skal anvendes), navnlig oplysninger, som lagres, behandles eller fremsendes elektronisk, uanset om oplysningerne er klassificerede eller uklassificerede.

TILRETTELÆGGELSE AF SIKKERHEDSBESKYTTELSEN

Fælles minimumsstandarder

8. Rådet og de enkelte medlemsstater sikrer, at alle administrative afdelinger, ministerier og styrelser, andre EU-institutioner, organer og tjenesteleverandører overholder fælles minimumsstandarder for sikkerhed, så EU-klassificerede oplysninger kan videregives i tillid til, at de vil blive sikret på tilsvarende måde. Disse minimumsstandarder skal omfatte kriterier for sikkerhedsgodkendelse af personale samt procedurer for beskyttelse af EU-klassificerede oplysninger.

MEDARBEJDERNE OG SIKKERHEDSBESKYTTELSEN

Sikkerhedsgodkendelse af medarbejdere

9. Alle medarbejdere, som skal have indsigt i oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, skal forinden være officielt sikkerhedsgodkendt. Tilsvarende skal der foretages forudgående sikkerhedsgodkendelse af personer, der skal stå for den tekniske drift eller vedligeholdelse af kommunikations- og informationssystemer, som indeholder klassificerede oplysninger. Meddelelse af sikkerhedsgodkendelse forudsætter, at de pågældende medarbejdere

a) er ubetinget pålidelige

b) har en sådan karakterstyrke og er så påpasselige, at der ikke kan herske tvivl om deres ubestikkelighed med hensyn til behandling af klassificerede oplysninger, og

c) ikke risikerer at blive udsat for pres fra udlandet eller anden side, f.eks. som følge af tidligere bopælsland eller tidligere tilhørsforhold, der kan udgøre en sikkerhedsrisiko.

Der skal foretages en særlig grundig sikkerhedsundersøgelse af medarbejdere, der:

d) skal have indsigt i oplysninger, som er klassificeret TRÈS SECRET UE/EU TOP SECRET

e) beklæder stillinger, som indebærer, at de regelmæssigt skal have indsigt i betydelige mængder af oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET

f) har særlig tjenstlig adgang til kommunikations- og informationssystemer med kritisk betydning for EU-operationer, og dermed ville have mulighed for at skaffe sig uautoriseret adgang til store mængder EU-klassificerede oplysninger eller for at forvolde de pågældende operationer betydelig skade gennem tekniske sabotagehandlinger.

▼B

I de i litra d), e) og f) nævnte tilfælde skal de pågældende medarbejderes personlige baggrund undersøges i videst muligt omfang.

10. Personer, for hvem indsigt ikke er tjenstlig nødvendig (f.eks. kontorbude, sikkerhedsvagter, vedligeholdelses- og rengøringspersonale), må ikke arbejde under forhold, hvor de kan få indsigt i EU-klassificerede oplysninger, medmindre de forinden er blevet sikkerhedsgodkendt til den relevante klassifikationsgrad.

Liste over sikkerhedsgodkendte personer

11. Alle tjenestegrene, styrelser mv., organer eller institutioner, der behandler EU-klassificerede oplysninger eller rummer kommunikations- og informationssystemer med kritisk betydning for EU-operationer, skal have en ajourført liste over deres sikkerhedsgodkendte medarbejdere. Hver enkelt sikkerhedsgodkendelse skal tages op til nyvurdering, når omstændighederne kræver det, for at sikre, at den svarer til den pågældendes aktuelle arbejdsopgaver; en sikkerhedsgodkendelse skal straks tages op til nyvurdering, hvis der fremkommer oplysninger, hvoraf det fremgår, at fortsat arbejde med klassificerede oplysninger ikke længere er foreneligt med hensynet til sikkerheden. Listen over sikkerhedsgodkendte medarbejdere føres af sikkerhedschefen for vedkommende tjenestegren, styrelse m.v. organ eller institution.

Sikkerhedsinstruks til medarbejderne

12. Alle medarbejdere, der varetager opgaver, hvor de kan få indsigt i klassificerede oplysninger, skal, inden de påbegynder arbejdet og derefter regelmæssigt, modtage en indgående instruks om nødvendigheden af sikkerhedsbeskyttelsen og procedurerne for gennemførelse af sikkerhedsbeskyttelsen. Det er hensigtsmæssigt at kræve, at de pågældende medarbejdere skriftligt attesterer, at de har forstået de sikkerhedsbestemmelser fuldt ud, der gælder for deres arbejdsopgaver.

Ledelsens ansvar

13. Det er ledelsens ansvar at vide, hvilke medarbejdere der behandler klassificerede oplysninger eller har adgang til kommunikations- og informationssystemer med kritisk betydning for EU-operationer, og at sikre, at alle former for hændelser eller klare svagheder, der kan have betydning for sikkerhedsbeskyttelsen, registreres og indberettes.

Medarbejdernes sikkerhedsstatus

14. Der indføres procedurer for at sikre, at hvis der fremkommer negative oplysninger om en medarbejder, bliver der taget stilling til, om den pågældende behandler klassificerede oplysninger eller har adgang til kommunikations- og informationssystemer med kritisk betydning for EU-operationer, og den relevante myndighed underrettes. Hvis det bekræftes, at medarbejderen udgør en sikkerhedsrisiko, må den pågældende ikke længere have adgang til oplysningerne og pålægges i stedet arbejdsopgaver, der ikke medfører nogen sikkerhedsrisiko.

FYSISK SIKKERHEDSBESKYTTELSE

Behovet for sikkerhedsbeskyttelse

15. Graden af de fysiske foranstaltninger, der skal bringes i anvendelse for at sikre beskyttelsen af EU-klassificerede oplysninger, skal stå i forhold til klassifikationsgraden samt omfanget af og truslen mod de oplysninger og det materiale, det drejer sig om. Man skal derfor søge at undgå, at der anvendes en for høj eller for lav klassificeringsgrad, og klassifikationsgraden skal regelmæssigt tages op til nyvurdering. Alle, der ligger inde med EU-klassificerede oplysninger, skal følge en ensartet praksis med hensyn til klassificering af de pågældende oplysninger og opfylde fælles standarder for sikkerhedsbeskyttelse for så vidt angår opbevaring, fremsendelse og bortskaffelse af oplysninger og materiale, der skal beskyttes.

Kontrol

16. Medarbejdere, der har modtaget EU-klassificerede oplysninger, må ikke efterlade disse uden opsigt, men skal sikre sig, at de opbevares forsvarligt, og at alle sikkerhedsanordninger er aktiveret (låse, alarmsystemer osv.). Herudover foretages der efter arbejdstids ophør kontrol af, om disse krav er opfyldt.

Sikkerhedsbeskyttelse af bygninger

17. Bygninger, der rummer EU-klassificerede oplysninger eller kommunikations- og informationssystemer med kritisk betydning for EU-operationer, skal beskyttes mod uautoriseret indsigt. Hvordan EU-klassificerede oplysninger skal beskyttes, med gitre for vinduer, låse på døre, vagtposter

▼B

ved indgange, automatiske adgangskontrolsystemer, sikkerhedskontrol og -patruljering, alarm- og overvågningssystemer, vagthunde m.v., afhænger af:

a) klassifikationsgraden af de oplysninger og det materiale, der skal beskyttes, samt deres omfang og placering i bygningen

b) kvaliteten af de penge- eller stålskabe m.v., hvor oplysningerne eller materialet opbevares, og

c) bygningens fysiske beskaffenhed og beliggenhed.

18. Hvordan kommunikations- og informationssystemer skal sikkerhedsbeskyttes, afhænger tilsvarende af en vurdering dels af værdien af de pågældende aktiver og den potentielle skade i tilfælde af brud på sikkerhedsbestemmelserne, dels af den fysiske beskaffenhed og beliggenhed af den bygning, der rummer systemet, dels af systemets placering i bygningen.

Beredskabsplaner

19. Der skal på forhånd udarbejdes detaljerede planer for, hvordan klassificerede oplysninger skal beskyttes, hvis der opstår en lokal eller landsomfattende kritisk situation.

INFORMATIONSSIKKERHED (INFOSEC)

20. INFOSEC defineres som identifikation og iværksættelse af sikkerhedsforanstaltninger, for at oplysninger, der behandles, lagres eller videregives via kommunikations-, informations- eller andre elektroniske systemer, kan sikres mod uagtsomt eller forsætligt at komme ikke-bemyndigede i hænde, samt mod ændring eller lækage. Der skal træffes fyldestgørende modforanstaltninger for at forhindre, at uautoriserede brugere får adgang til EU-oplysninger, og at autoriserede brugere ikke får adgang til EU-oplysninger, samt forebygge, at EU-oplysninger forvanskes, eller at de ændres eller slettes uden bemyndigelse.

BEKÆMPELSE AF SABOTAGE OG ANDRE FORMER FOR FORSÆTLIG SKADE

21. Fysiske forholdsregler til beskyttelse af vigtige anlæg med klassificerede oplysninger er de mest egnede sikkerhedsforanstaltninger, der kan træffes mod sabotage og anden forsætlig skade, og sikkerhedsgodkendelse af personalet er i sig selv ikke nok. Vedkommende nationale sikkerhedsmyndigheder indsamler efterretninger om spionage, sabotage, terrorisme og anden undergravende virksomhed.

VIDEREGIVELSE AF KLASSIFICEREDE OPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

22. Beslutninger om, at EU-klassificerede oplysninger, der er udstedt af Rådet, skal videregives til et tredjeland eller en international organisation, træffes af Rådet. Hvis de oplysninger, der ønskes videregivet, ikke er udstedt af Rådet, skal Rådet først indhente udstederens samtykke til videregivelsen. Hvis det ikke kan fastslås, hvem udstederen er, påtager Rådet sig dennes ansvar.

23. Modtager Rådet klassificerede oplysninger fra tredjelande, internationale organisationer eller anden tredjepart, skal de pågældende oplysninger beskyttes i overensstemmelse med deres klassifikationsgrad og de standarder, der ifølge denne afgørelse gælder for EU-klassificerede oplysninger, eller eventuelt højere standarder, som den tredjepart, der videregiver oplysningerne, måtte stille krav om. Der kan åbnes mulighed for gensidige kontrol.

24. Ovennævnte principper gennemføres i overensstemmelse med de nærmere bestemmelser i del II.

▼B

DEL II

AFSNIT I

KOMPETENCEFORDELINGEN FOR SIKKERHEDSBESKYTTELSE I RÅDET FOR DEN EUROPÆISKE UNION

Generalsekretæren/den højtstående repræsentant

1. Generalsekretæren/den højtstående repræsentant skal:

   a) gennemføre Rådets sikkerhedspolitik

   b) tage stilling til sikkerhedsproblemer, der forelægges ham af Rådet eller dets kompetente organer

   c) behandle spørgsmål, der indebærer ændringer i Rådets sikkerhedspolitik, i tæt kontakt med medlemsstaternes nationale sikkerhedsmyndigheder (eller andre relevante myndigheder). Tillæg 1 indeholder en liste over disse myndigheder.

2. Generalsekretæren/den højtstående repræsentant er navnlig ansvarlig for:

   a) at samordne alle sikkerhedsspørgsmål, der vedrører Rådets virksomhed

   b) at henstille, at hver medlemsstat opretter et centralt sekretariat for oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, og kræve, at et sådant sekretariat ligeledes oprettes i EU's decentrale organer, hvor det er relevant

   c) at anmode de af medlemsstaterne udpegede myndigheder om, at de nationale sikkerhedsmyndigheder foretager sikkerhedsgodkendelse af personale, der arbejder i GSR, jf. afgørelsen i afsnit VI

   d) at iværksætte en undersøgelse eller foranledige en undersøgelse iværksat i eventuelle tilfælde af uautoriseret videregivelse af EU-klassificerede oplysninger, der umiddelbart forekommer at være sket i GSR eller et af EU's decentrale organer

   e) at anmode de relevante sikkerhedsmyndigheder om at iværksætte efterforskning, hvis uautoriseret videregivelse af EU-klassificerede oplysninger forekommer at være sket uden for GSR eller EU's decentrale organer, og samordne efterforskningen, hvis mere end én sikkerhedsmyndighed er involveret

   f) sammen med og i forståelse med de pågældende nationale sikkerhedsmyndigheder at foretage regelmæssig gennemgang af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger i medlemsstaterne

   g) at holde løbende kontakt til vedkommende sikkerhedsmyndigheder med henblik på at varetage den overordnede samordning af sikkerhedsbeskyttelsen

   h) løbende at tage Rådets sikkerhedspolitik og -procedurer op til nyvurdering og at udarbejde relevante henstillinger. Han forelægger i den forbindelse Rådet den årlige inspektionsplan, der udarbejdes af GSR's Sikkerhedskontor.

Rådets Sikkerhedsudvalg

3. Der oprettes et sikkerhedsudvalg sammensat af repræsentanter for de enkelte medlemsstaters nationale sikkerhedsmyndigheder og med generalsekretæren/den højtstående repræsentant eller en af denne udpeget stedfortræder som formand. Repræsentanter for EU's decentrale organer kan ligeledes opfordres til at deltage, hvis der skal drøftes spørgsmål, som berører dem.

4. Sikkerhedsudvalget træder sammen efter Rådets anvisninger på anmodning af generalsekretæren/den højtstående repræsentant eller en national sikkerhedsmyndighed. Det har beføjelse til at behandle og vurdere alle sikkerhedsspørgsmål i forbindelse med Rådets arbejde og til at forelægge Rådet relevante indstillinger. For så vidt angår GSR's virksomhed har udvalget beføjelse til at forelægge generalsekretæren/den højtstående repræsentant relevante indstillinger vedrørende sikkerhedsspørgsmål.

Sikkerhedskontoret ved Generalsekretariatet for Rådet

5. Med henblik på udførelsen af de opgaver, der er nævnt i nr. 1 og 2 ovenfor, kan generalsekretæren/den højtstående repræsentant pålægge GSR's Sikkerhedskontor at samordne, føre tilsyn med og gennemføre sikkerhedsforanstaltninger.

▼B

6. Chefen for GSR's Sikkerhedskontor er generalsekretærens/den højtstående repræsentants ledende konsulent i sikkerhedsspørgsmål og fungerer som Sikkerhedsudvalgets sekretær. I denne forbindelse forestår han ajourføringen af sikkerhedsforskrifterne og samordner sikkerhedsforanstaltningerne med medlemsstaternes myndigheder samt i relevant omfang med internationale organisationer, der har sikkerhedsaftaler med Rådet. Med henblik herpå fungerer han som forbindelsesofficer.

7. Chefen for GSR's Sikkerhedskontor er ansvarlig for godkendelsen af IT-systemer og -netværk i GSR. Chefen for GSR's Sikkerhedskontor og vedkommende nationale sikkerhedsmyndighed træffer, hvor det er relevant, i fællesskab beslutning om godkendelsen af IT-systemer og -netværk, der berører GSR, medlemsstaterne, EU's decentraliserede organer og/eller tredjeparter (lande eller internationale organisationer).

EU's decentraliserede organer

8. Direktøren for hvert af EU's decentrale organer er ansvarlig for gennemførelsen af sikkerhedsbeskyttelsen i det pågældende organ. Direktøren udpeger normalt en af sine medarbejdere som ansvarlig over for direktøren på dette område. Denne medarbejder udpeges som det decentrale organs sikkerhedsofficer.

Medlemsstaterne

9. Hver medlemsstat udpeger en national sikkerhedsmyndighed med ansvar for beskyttelse af EU-klassificerede oplysninger ([1]).

10. Inden for de enkelte medlemsstaters forvaltninger er den nationale sikkerhedsmyndighed ansvarlig for:

    a) beskyttelse af EU-klassificerede oplysninger, der opbevares af ministerier, styrelser m.v. eller offentlige såvel som private organer, i ind- eller udland

    b) at give bemyndigelse til oprettelse af registre over oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET (denne bemyndigelse kan delegeres til et centralt sekretariats kontrolansvarlige for oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET)

    c) regelmæssig inspektion af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger

    d) at sikre, at alle landets egne statsborgere samt alle udlændinge, der arbejder i nationale ministerier, organer eller myndigheder, som har direkte adgang til oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE, er blevet sikkerhedsgodkendt

    e) at udarbejde de sikkerhedsplaner, der skønnes nødvendige for at forhindre uautoriseret indsigt i EU-klassificerede oplysninger.

Gensidige sikkerhedsinspektioner

11. GSR's Sikkerhedskontor og vedkommende nationale sikkerhedsmyndighed gennemfører i fællesskab og efter fælles aftale regelmæssige inspektioner af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger i GSR og i medlemsstaternes faste repræsentationer ved Den Europæiske Union samt i medlemsstaternes lokaler i Rådets bygninger ([2]).

12. GSR's Sikkerhedskontor eller, på anmodning af generalsekretæren/den højtstående repræsentant, værtsmedlemsstatens nationale sikkerhedsmyndighed gennemfører regelmæssige inspektioner af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger i EU's decentraliserede organer.

([1]) En liste over de nationale sikkerhedsmyndigheder med ansvar for beskyttelse af EU-klassificerede oplysninger findes i tillæg 1.
([2]) Med forbehold af Wienerkonventionen af 1961 om diplomatiske forbindelser.

▼B

AFSNIT II

KLASSIFIKATIONSGRAD OG ANDEN PÅTEGNING

KLASSIFIKATIONSGRADER ([1])

Oplysninger klassificeres således:

1. TRÈS SECRET UE/EU TOP SECRET: Denne klassifikation anvendes kun til oplysninger og materiale, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Den Europæiske Unions eller én eller flere af dens medlemsstaters vitale interesser overordentlig alvorlig skade.

2. SECRET UE: Denne klassifikation anvendes kun til oplysninger og materiale, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Den Europæiske Unions eller én eller flere af dens medlemsstaters vitale interesser alvorlig skade.

3. CONFIDENTIEL UE: Denne klassifikation anvendes til oplysninger og materiale, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Den Europæiske Unions eller en eller flere af dens medlemsstaters vitale interesser skade.

4. RESTREINT UE: Denne klassifikation anvendes til oplysninger og materiale, hvis videregivelse uden dertil indhentet bemyndigelse vil være uhensigtsmæssig for Den Europæiske Unions eller en eller flere af dens medlemsstaters interesser.

ANDEN PÅTEGNING

5. Det kan med en særlig påtegning angives, hvilket område dokumentet omhandler, eller hvordan det skal fordeles efter »need-to-know«-princippet.

6. Betegnelsen ESDP/PESD kan anføres på dokumenter eller kopier deraf, som vedrører EU's eller en eller flere af dets medlemsstaters sikkerhed eller forsvar, eller som vedrører militær eller ikke-militær krisestyring.

7. Herudover kan visse dokumenter, navnlig vedrørende IT-systemer, forsynes med en påtegning om yderligere sikkerhedsforanstaltninger i henhold til relevante bestemmelser.

ANFØRING AF KLASSIFIKATIONSGRAD

8. Klassifikationsgraden anføres således:

   a) på dokumenter, der er klassificeret RESTREINT UE: mekanisk eller elektronisk

   b) på dokumenter, der er klassificeret CONFIDENTIEL UE: mekanisk eller i hånden eller ved fortryk på registreret papir

   c) på dokumenter, der er klassificeret SECRET UE eller TRÈS SECRET UE/EU TOP SECRET: mekanisk eller i hånden.

([1]) En sammenlignende oversigt over EU's, NATO's, WEU's og medlemsstaternes klassifikationsgrader findes i tillæg 2.

▼B

AFSNIT III

KLASSIFIKATIONSSTYRING

1. Oplysninger klassificeres kun i nødvendigt omfang. Klassifikationsgraden skal fremgå klart og korrekt, og den gælder kun, så længe der er grund til at beskytte oplysningerne.

2. Ansvaret for klassificering af oplysninger og for eventuel senere nedklassificering eller afklassificering ([1]) påhviler alene udstederen.

   Tjenestemænd og øvrige ansatte ved GSR klassificerer, nedklassificerer eller afklassificerer oplysninger efter instruks fra eller aftale med deres generaldirektør.

3. De detaljerede procedurer for behandling af klassificerede dokumenter er udformet således, at det sikres, at dokumenterne beskyttes i overensstemmelse med de oplysninger, de indeholder.

4. Antallet af medarbejdere, der er berettiget til at udstede dokumenter med klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET, skal holdes på et minimum, og deres navne skal stå på en liste, der udarbejdes af GSR, hver medlemsstat samt i relevant omfang hvert af EU's decentrale organer.

ANVENDELSE AF KLASSIFICERING

5. Klassificeringen af et dokument afhænger af, hvor følsomt dets indhold er, jf. definitionen i afsnit II, punkt 1-4. Det er vigtigt, at oplysninger klassificeres korrekt, og at klassificering ikke overdrives. Dette gælder navnlig anvendelse af klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET.

6. Når et dokument klassificeres, skal udstederen være opmærksom på ovennævnte bestemmelser og bremse enhver tendens til at anvende for høj eller for lav klassifikationsgrad.

   Selv om en høj klassifikationsgrad umiddelbart kunne tænkes at sikre et dokument større beskyttelse, kan rutinemæssig anvendelse af en for høj klassifikationsgrad nedsætte tilliden til klassifikationsordningen.

   På den anden side må dokumenter ikke klassificeres for lavt blot for at undgå de begrænsninger, de enkelte klassifikationsgrader medfører.

   En praktisk klassifikationsvejledning findes i tillæg 3.

7. De enkelte sider, afsnit og punkter i et dokument samt bilag, tillæg og vedhæftet materiale kan kræve forskellig klassifikationsgrad, hvilket skal fremgå tydeligt. Dokumentet som helhed skal dog have samme klassifikationsgrad som den del, der har den højeste klassifikationsgrad.

8. En følgeskrivelse klassificeres i overensstemmelse med bilagenes højeste klassifikationsgrad. Dokumentets udsteder bør klart angive, på hvilket niveau følgeskrivelsen skal klassificeres, hvis den adskilles fra bilaget.

NEDKLASSIFICERING OG AFKLASSIFICERING

9. EU-klassificerede dokumenter må kun nedklassificeres eller afklassificeres med udstederens tilladelse og om nødvendigt efter drøftelse med andre berørte parter. Nedklassificeringen eller afklassificeringen skal bekræftes skriftligt. Den institution eller medlemsstat, den styrelse eller afdeling, den efterfølgende organisation eller højere myndighed, der har udstedt dokumentet, er ansvarlig for at underrette dokumentets modtagere om ændringen, og disse er på deres side ansvarlige for at underrette efterfølgende modtagere, til hvem de har sendt eller kopieret dokumentet, om ændringen.

10. Så vidt muligt anfører udstederen på de klassificerede dokumenter en dato eller frist, efter hvilken indholdet kan nedklassificeres eller afklassificeres. I modsat fald skal vedkommende tage klassificeringen op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig.

([1]) Ved nedklassificering (»downgrading«) forstås anvendelse af en lavere klassifikationsgrad; ved afklassificering (»declassification«) forstås ophævelse af enhver form for klassificering.

▼B

AFSNIT IV

FYSISK SIKKERHEDSBESKYTTELSE

GENERELT

1. Hovedformålet med fysiske sikkerhedsforanstaltninger er at forhindre uautoriseret adgang til EU-klassificerede oplysninger og/eller EU-klassificeret materiale.

SIKKERHEDSKRAV

2. Alle lokaliteter, områder, bygninger, kontorer, lokaler, kommunikations- og informationssystemer m.v., hvor der opbevares og/eller behandles EU-klassificerede oplysninger og EU-klassificeret materiale, skal beskyttes ved hjælp af passende fysiske sikkerhedsforanstaltninger.

3. Når det skal afgøres, hvilken grad af fysisk sikkerhedsbeskyttelse der er nødvendigt, skal der tages hensyn til alle relevante faktorer som f.eks.:

   a) oplysningernes og/eller materialets klassifikationsgrad

   b) oplysningernes mængde og form (f.eks. på papir eller i elektronisk form)

   c) vedkommende efterretningstjenesters vurdering af den lokale trussel mod EU, medlemsstaterne og/eller andre institutioner eller tredjeparter, der ligger inde med EU-klassificerede oplysninger, navnlig med hensyn til risiko for sabotage, terrorisme, undergravende og/eller anden kriminel virksomhed.

4. De fysiske sikkerhedsforanstaltninger, der bringes i anvendelse, skal tage sigte på:

   a) at forhindre, at uautoriserede personer ubemærket kan få adgang eller kan tiltvinge sig adgang til de pågældende oplysninger

   b) at forebygge, vanskeliggøre og i givet fald afsløre handlinger fra upålidelige medarbejderes side (»muldvarpe«)

   c) at forhindre, at medarbejdere ved GSR, medlemsstaternes ministerier, styrelser m.v. og/eller andre institutioner eller tredjeparter, for hvem indsigt ikke er tjenstlig nødvendig, får adgang til EU-klassificerede oplysninger.

FYSISKE SIKKERHEDSFORANSTALTNINGER

Sikkerhedszoner

5. Zoner, hvor oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, behandles eller opbevares, skal være således struktureret og indrettet, at de opfylder kravene for en af følgende klasser:

   a) Sikkerhedszone af klasse I: zone, hvor oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, behandles eller opbevares på en sådan måde, at personer, der har adgang til zonen, uden videre også har adgang til de klassificerede oplysninger. Zonen skal:

      i) være tydeligt afgrænset og sikret, og al ind- og udgang skal kontrolleres

      ii) have et adgangskontrolsystem, så der kun er adgang for særligt autoriserede medarbejdere

      iii) ved tydelig skiltning vise, hvilken klassifikationsgrad af oplysninger, der normalt opbevares i zonen, dvs. hvilke oplysninger man får adgang til ved at komme ind i zonen

   b) Sikkerhedszone af klasse II: zone, hvor oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, behandles eller opbevares på en sådan måde, at medarbejdere, der ikke er berettiget til at få indsigt i oplysningerne, kan forhindres ved hjælp af intern kontrol i at komme ind på områder med kontorer m.v., hvor oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, normalt behandles eller opbevares. Zonen skal:

      i) være tydeligt afgrænset og sikret, og al ind- og udgang skal kontrolleres

      ii) have et adgangskontrolsystem, så der kun er adgang uden ledsagelse for særligt autoriserede medarbejdere med relevant sikkerhedsgodkendelse. Alle andre personer skal ledsages eller på anden måde forhindres i at få uautoriseret adgang til EU-klassificerede oplysninger eller ukontrolleret adgang til zoner, som er omfattet af teknisk sikkerhedsinspektion.

▼B

Zoner, hvortil vagter ikke døgnet rundt kontrollerer adgangen, skal inspiceres umiddelbart efter normal arbejdstids ophør for at sikre, at EU-klassificerede oplysninger opbevares efter sikkerhedsforskrifterne.

Administrativ zone

6. Der kan oprettes en administrativ zone med et lavere sikkerhedsniveau rundt om eller foran sikkerhedszoner af klasse I eller klasse II. En sådan zone skal være tydeligt afgrænset, så personer og køretøjer kan kontrolleres. I administrative zoner må der ikke behandles eller opbevares oplysninger, der er klassificeret højere end RESTREINT UE.

Adgangskontrol

7. Adgang til sikkerhedszoner af klasse I og II kontrolleres ved hjælp af adgangsbadge eller et personligt identifikationssystem for de fastemedarbejdere. Der indføres tillige et kontrolsystem for besøgende; dette udformes således, at uautoriserede personer ikke kan få adgang til EU-klassificerede oplysninger. Adgangsbadgeordningen kan suppleres med automatiseret identifikation, der skal betragtes som et supplement til vagternes visuelle kontrol, men ikke fuldstændig kan træde i stedet for en sådan kontrol. En ændret trusselsvurdering kan betyde, at der må indføres skærpet adgangskontrol, f. eks. i forbindelse med VIP-besøg.

Rundering

8. I sikkerhedszoner af klasse I og II gennemføres rundering uden for normal arbejdstid for at beskytte EU's aktiver mod lækage, skade eller tab. Rundering foretages så ofte, som de stedlige omstændigheder kræver det eller hver anden time.

Bokslokaler, penge- eller stålskabe, m.v.

9. Der anvendes tre klasser af sikrede bokslokaler, penge- eller stålskabe m.v. til opbevaring af oplysninger med EU-klassifikation:

   — Klasse A: bokslokaler, penge- eller stålskabe m.v., som er godkendt på nationalt plan til opbevaring af oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, i en sikkerhedszone af klasse I eller II

   — Klasse B: bokslokaler, penge- eller stålskabe m.v., som er godkendt på nationalt plan til opbevaring af oplysninger, der er klassificeret SECRET UE eller CONFIDENTIEL UE i en sikkerhedszone af klasse I eller II

   — Klasse C: kontormøbler, hvori der ikke må opbevares oplysninger, hvis de er klassificeret højere end RESTREINT UE.

10. I bokslokaler, der indrettes inde i en sikkerhedszone af klasse I eller II og i alle sikkerhedszoner af klasse I, hvor der på åbne reoler eller plottet ind på kort m.v. opbevares oplysninger, som er klassificeret CONFIDENTIEL UE eller højere, skal vægge, gulve og lofter samt dør(e) og låsemekanismer være godkendt af den nationale sikkerhedsmyndighed, som attesterer, at lokalerne yder samme beskyttelse som den type bokslokale, penge- eller stålskab m.v., der er godkendt til opbevaring af oplysninger med samme klassifikationsgrad.

Låsemekanismer

11. De låsemekanismer, der anvendes til bokslokaler, penge- eller stålskabe m. v., hvori der opbevares EU-klassificerede oplysninger, skal opfylde følgende krav:

   — Gruppe A: godkendt på nationalt plan til bokslokaler, penge- eller stålskabe m.v. af klasse A

   — Gruppe B: godkendt på nationalt plan til bokslokaler, penge- eller stålskabe m.v. af klasse B

   — Gruppe C: kun egnet til kontormøbler af klasse C.

Kontrol med nøgler og koder

12. Nøgler til bokslokaler, penge- eller stålskabe m.v. må ikke tages med uden for kontorbygningen. Medarbejdere, for hvem det er tjenstlig nødvendigt at kende en evt. adgangskode, skal lære denne udenad. Vedkommende sikkerhedsofficer har ansvaret for at opbevare reservenøgler samt en skriftlig fortegnelse over alle koderne, som kan anvendes, hvis der opstår en nødsituation; koderne skal opbevares for sig i forseglede uigennemsigtige kuverter. Arbejdsnøgler, reservesikkerhedsnøgler og koder skal opbevares hver for sig i penge- eller stålskabe m.v. Nøgler eller koder må ikke have et lavere beskyttelsesniveau end det materiale, de giver adgang til.

▼B

13. Så få medarbejdere som muligt skal have kendskab til koderne til penge- eller stålskabe m.v. Koderne ændres:

    a) hver gang der modtages et nyt penge- eller stålskab m.v.

    b) hver gang en medarbejder fratræder, og hver gang en ny medarbejder tiltræder

    c) hvis oplysninger er lækket, eller der er mistanke om, at oplysninger er lækket

    d) om muligt hver sjette måned, dog mindst en gang om året.

Anordninger til afsløring af uvedkommendes forsøg på at skaffe sig adgang

14. Anvendes der alarmsystemer, kameraovervågning eller andre elektriske anordninger for at beskytte EU-klassificerede oplysninger, skal der være en nød-elforsyning, som sikrer systemets fortsatte drift, hvis hoved-elforsyningen afbrydes. Et andet grundlæggende krav er, at alarmen skal udløses, eller at vagterne på anden pålidelig måde skal alarmeres, hvis der opstår fejl i systemets drift, eller hvis der forsøges foretaget ulovlige indgreb i det.

Godkendt udstyr

15. Den nationale sikkerhedsmyndighed ajourfører ud fra egne eller bilaterale kilder fortegnelser over de typer og modeller af sikkerhedsudstyr, den har godkendt til direkte eller indirekte beskyttelse af klassificerede oplysninger under forskellige nærmere angivne omstændigheder og vilkår. GSR's sikkerhedskontor fører en tilsvarende fortegnelse, blandt andet på grundlag af oplysninger fra de nationale sikkerhedsmyndigheder. Decentrale EU-organer skal høre GSR's sikkerhedskontor og eventuelt værtslandets nationale sikkerhedsmyndighed inden anskaffelse af sådant udstyr.

Fysisk beskyttelse af kopi- og telefaxmaskiner

16. Kopi- og telefaxmaskiner beskyttes fysisk i det omfang, det er nødvendigt for at sikre, at de kun kan anvendes af autoriserede medarbejdere, og at der føres den nødvendige kontrol med alt klassificeret materiale.

BESKYTTELSE MOD UVEDKOMMENDES BLIKKE OG AFLYTNING

Uvedkommendes blikke

17. Der træffes alle nødvendige foranstaltninger til at sikre, at uvedkommende ikke på noget tidspunkt af døgnet kan få lejlighed til at se EU-klassificerede oplysninger, end ikke ved et tilfælde.

Aflytning

18. Kontorer eller zoner, hvor der regelmæssigt drøftes anliggender, der er klassificeret SECRET UE (hemmeligt) eller højere, beskyttes mod aktiv og passiv aflytning i det omfang en risikovurdering tilsiger det. Det påhviler vedkommende sikkerhedsmyndighed at vurdere risikoen for aflytning, om nødvendigt efter at have hørt nationale sikkerhedsmyndigheder.

19. Med henblik på fastsættelse af de beskyttelsesforanstaltninger, der skal træffes i bygninger, hvor det er vigtigt at undgå dels passiv aflytning (f. eks. isolering af vægge, døre, gulve og lofter og måling af, hvor meget man kan høre udenfor) og dels aktiv aflytning (f.eks. detektion af skjulte mikrofoner), kan GSR's sikkerhedskontor anmode om bistand fra de nationale sikkerhedsmyndigheder. Decentrale EU-organers sikkerhedsofficer kan anmode GSR's sikkerhedskontor om at udføre tekniske inspektioner og/eller anmode om bistand fra nationale sikkerhedsmyndigheders eksperter.

20. Når omstændighederne tilsiger det, kan sikkerhedsteknikere fra nationale sikkerhedsmyndigheder på vedkommende sikkerhedsofficers anmodning ligeledes inspicere telekommunikationsudstyr og det elektriske eller elektroniske kontormateriel, der anvendes under møder, hvor drøftelserne er klassificeret SECRET UE eller højere.

TEKNISK SIKREDE ZONER

21. Visse zoner kan udpeges som teknisk sikrede zoner. Der foretages en særlig adgangskontrol. Når disse zoner ikke bruges, skal de holdes aflåst ved hjælp af en godkendt procedure, og alle nøgler skal betragtes som sikkerhedsnøgler. Der foretages regelmæssig fysisk inspektion af sådanne zoner, og inspektion foretages ligeledes, hvis uvedkommende har fået adgang til zonerne, eller hvis der er mistanke om, at uvedkommende har fået adgang.

22. Der udarbejdes en detaljeret fortegnelse over materiel og møblement, så der kan føres kontrol med, i hvilket lokale det hører hjemme. Intet møbel eller udstyr må bringes ind i disse zoner, uden at det først er blevet nøje inspiceret af særligt uddannet sikkerhedspersonale med henblik på

▼B

detektion af aflytningsudstyr. Det bør normalt undgås at installere kommunikationslinjer i teknisk sikrede zoner.

▼B

AFSNIT V

ALMINDELIGE BESTEMMELSER OM »NEED-TO-KNOW«-PRINCIPPET OG SIKKERHEDSGODKENDELSE

1. Kun personer, for hvem indsigt er tjenstlig nødvendig (»need-to-know«), må få indsigt i EU klassificerede oplysninger. Oplysninger, der er klassificeret TRÈS SECRET/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE, må kun komme personer i hænde, der er sikkerhedsgodkendt til den pågældende klassifikationsgrad.

2. Det påhviler GSR, de decentrale EU-organer eller vedkommende myndigheder i den medlemsstat, hvor en ny medarbejder skal tiltræde, at træffe afgørelse om, hvilke oplysninger den pågældende har tjenstligt behov for at få kendskab til, alt efter de arbejdsopgaver, der vil blive pålagt.

3. Arbejdsgiveren er ansvarlig for, at medarbejderne er sikkerhedsgodkendt efter de relevante procedurer. For så vidt angår GSR's tjenestemænd og øvrige ansatte anvendes proceduren for sikkerhedsgodkendelse i afsnit VI.

   Der vil derefter blive udstedt et »sikkerhedscertifikat« med angivelse af den højeste klassifikationsgrad den godkendte har adgang til, samt udløbsdatoen for godkendelsen.

   Et sikkerhedscertifikat til en bestemt klassifikationsgrad gælder ligeledes for adgang til oplysninger med lavere klassifikationsgrad.

4. Hvis det er nødvendigt at drøfte EU-klassificerede oplysninger med personer, som ikke er tjenestemænd eller andre ansatte i GSR eller medlemsstaternes egne medarbejdere, men f.eks. er medlemmer af eller tjenestemænd eller andre ansatte ved EU's øvrige institutioner, eller det er nødvendigt at vise dem sådanne oplysninger, skal de pågældende først være sikkerhedsgodkendt til EU-klassificerede oplysninger, og de skal orienteres om deres sikkerhedsmæssige ansvar. Samme regel gælder under tilsvarende omstændigheder for eksterne kontrahenter, eksperter eller konsulenter.

SÆRBESTEMMELSER OM INDSIGT I OPLYSNINGER, DER ER KLASSIFICERET TRÈS SECRET UE/EU TOP SECRET

5. Enhver, der skal have indsigt i oplysninger, som er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal først være sikkerhedsgodkendt til denne klassifikationsgrad.

6. Enhver, der skal have indsigt i oplysninger, som er klassificeret TRÈS SECRET UE/EU TOP SECRET, udpeges af chefen for den pågældende afdeling eller styrelse, og deres navn skal optages på listen over de medarbejdere, der er sikkerhedsgodkendt til TRÈS SECRET UE/EU TOP SECRET.

7. Enhver, der skal have indsigt i oplysninger, som er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal forinden underskrive en erklæring om at være blevet orienteret om Rådets sikkerhedsprocedurer og fuldt ud at have forstået sit særlige ansvar for at beskytte oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, samt konsekvenserne i henhold til EU-bestemmelser og medlemsstaternes love eller administrative bestemmelser, såfremt uvedkommende med forsæt eller uagtsomt får adgang til klassificerede oplysninger.

8. Hvis en medarbejder skal deltage i møder o.l., hvor den pågældende vil få adgang til oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal sikkerhedsofficeren i den styrelse eller afdeling, hvor medarbejderen er ansat, meddele den instans, som afholder mødet, at medarbejderen har den nødvendige sikkerhedsgodkendelse.

9. Navnene på samtlige personer, hvis arbejdsopgaver ikke længere kræver indsigt i oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal fjernes fra TRÈS SECRET UE/EU TOP SECRET-listen. Derudover skal de pågældende gøres opmærksom på deres særlige ansvar for beskyttelse af de oplysninger, de er blevet bekendt med, og som er klassificeret TRÈS SECRET/EU TOP SECRET. De skal desuden underskrive en erklæring om, at de hverken vil bruge eller videregive oplysninger i deres besiddelse, der er klassificeret TRÈS SECRET UE/EU TOP SECRET.

SÆRBESTEMMELSER OM INDSIGT I OPLYSNINGER, DER ER KLASSIFICERET SECRET UE ELLER CONFIDENTIEL UE

10. Enhver, der skal have indsigt i oplysninger, som er klassificeret SECRET UE eller CONFIDENTIEL UE, skal først være sikkerhedsgodkendt til den pågældende klassifikationsgrad.

▼B

11. Enhver, der skal have indsigt i oplysninger, som er klassificeret SECRET UE eller CONFIDENTIEL UE, skal gøres bekendt med de relevante sikkerhedsbestemmelser og skal være klar over konsekvenserne af uagtsomhed.

12. Hvis en medarbejder skal deltage i møder o.l., hvor den pågældende vil få adgang til oplysninger, der er klassificeret SECRET UE eller CONFIDENTIEL UE, skal sikkerhedsofficeren i den styrelse eller afdeling, hvor medarbejderen er ansat, meddele den instans, der afholder mødet, at medarbejderen har den nødvendige sikkerhedsgodkendelse.

SÆRBESTEMMELSER OM INDSIGT I OPLYSNINGER, DER ER KLASSIFICERET RESTREINT UE

13. Alle, der har indsigt i oplysninger, som er klassificeret RESTREINT UE, gøres bekendt med disse sikkerhedsforskrifter og konsekvenserne af uagtsomhed.

OVERDRAGELSE AF MATERIALE

14. Hvis en medarbejder skal gøre tjeneste andetsteds efter at have behandlet EU-klassificeret materiale og afløses af en anden, påser vedkommende sekretariat, at det klassificerede materiale overdrages korrekt fra den fratrædende til den tiltrædende medarbejder.

SÆRLIGE INSTRUKSER

15. Personer, som tjenstlig skal have indsigt i EU-klassificerede oplysninger, bør ved tildelingen af sådanne arbejdsopgaver og med regelmæssige mellemrum derefter gøres opmærksom på:

    a) sikkerhedsrisikoen ved uoverlagt tale

    b) forholdsregler over for pressen

    c) truslen fra efterretningstjenester, der opererer i EU og medlemsstaterne med henblik på at indsamle oplysninger og følge aktiviteter, der er EU-klassificerede

    d) pligten til straks at rapportere til vedkommende sikkerhedsmyndigheder om enhver henvendelse eller handling, der kan vække mistanke om spionage, eller enhver usædvanlig sikkerhedsrelevant omstændighed.

16. Enhver, der normalt er i hyppig kontakt med repræsentanter for lande, hvis efterretningstjenester opererer i EU og medlemsstaterne med henblik på at indsamle oplysninger og følge aktiviteter, der er EU-klassificerede, skal orienteres om de teknikker, sådanne efterretningstjenester vides at benytte sig af.

17. Rådet har ingen sikkerhedsbestemmelser vedrørende private rejser, som foretages af medarbejdere, der er sikkerhedsgodkendt til EU-klassificerede oplysninger. Vedkommende sikkerhedsmyndigheder gør imidlertid sådanne medarbejdere bekendt med de rejsebestemmelser, de inden for deres ansvarsområde er omfattet af. Sikkerhedsofficeren drager omsorg for, at der afholdes genopfriskningskurser for medarbejderne vedrørende sådanne særbestemmelser.

▼B

AFSNIT VI

AFGØRELSE OM SIKKERHEDSGODKENDELSE AF TJENESTEMÆND OG ØVRIGE ANSATTE I GSR

1. Kun tjenestemænd og øvrige ansatte i GSR eller personer, der arbejder i GSR, og som i embeds medfør og af tjenstlige grunde har brug for at få kendskab til eller behandle klassificerede oplysninger i Rådets besiddelse, kan få adgang til sådanne oplysninger.

2. For at få indsigt i oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE, skal de i nr. 1 omhandlede personer først godkendes til den pågældende klassifikationsgrad efter proceduren i nr. 4 og 5.

3. Godkendelsen gives kun til personer, der er blevet sikkerhedsundersøgt af medlemsstaternes kompetente nationale myndigheder (den nationale sikkerhedsmyndighed) efter proceduren i nr. 6-10.

4. Ansættelsesmyndigheden som defineret i personalevedtægtens artikel 2, stk. 1, meddeler de i nr. 1, 2 og 3 omhandlede godkendelser.

   Ansættelsesmyndigheden meddeler godkendelsen efter at have indhentet udtalelse fra medlemsstaternes kompetente nationale myndigheder på grundlag af sikkerhedsundersøgelsen i henhold til nr. 6-12.

5. Godkendelsen er gyldig i fem år, dog ikke længere end varigheden af de arbejdsopgaver, der ligger til grund for den. Gyldighedsperioden kan forlænges af ansættelsesmyndigheden efter proceduren i nr. 4.

   Ansættelsesmyndigheden kan dog inddrage godkendelsen, såfremt den finder, at der er grund hertil. Ansættelsesmyndigheden giver underretning om inddragelsen til den pågældende person, der kan anmode om at måtte fremsætte sine bemærkninger over for ansættelsesmyndigheden, samt til de kompetente nationale myndigheder.

6. Sikkerhedsundersøgelsen har til formål at sikre, at der ikke er noget til hinder for, at den pågældende person kan få adgang til klassificerede oplysninger i Rådets besiddelse.

7. Sikkerhedsundersøgelsen foretages med den berørte persons medvirken og efter anmodning fra ansættelsesmyndigheden; undersøgelsen foretages af de kompetente myndigheder i den medlemsstat, hvor den person, der skal sikkerhedsgodkendes, er statsborger. Såfremt den pågældende person er bosiddende på en anden medlemsstats område, kan de kompetente nationale myndigheder sikre sig bopælsstatens myndigheders samarbejde.

8. Den pågældende skal med henblik på sikkerhedsundersøgelsen udfylde et skema med angivelse af personlige oplysninger.

9. Ansættelsesmyndigheden giver i sin anmodning nærmere oplysninger om arten af og klassifikationsniveauet for de oplysninger, som den pågældende person vil få kendskab til, så de kompetente nationale myndigheder kan foretage sikkerhedsundersøgelsen og afgive en udtalelse om den pågældendes relevante godkendelsesniveau.

10. De forskrifter og bestemmelser vedrørende sikkerhedsundersøgelse, som er gældende i vedkommende medlemsstat, herunder forskrifter og bestemmelser om eventuel klageadgang, finder anvendelse i forbindelse med hele sikkerhedsundersøgelsens forløb og dens resultater.

11. Såfremt medlemsstaternes kompetente nationale myndigheder afgiver positiv udtalelse, kan ansættelsesmyndigheden godkende den pågældende person.

12. Såfremt de kompetente nationale myndigheder afgiver negativ udtalelse, underrettes den pågældende person om udtalelsens resultat, og vedkommende kan anmode om at måtte fremsætte sine bemærkninger over for ansættelsesmyndigheden. Hvis ansættelsesmyndigheden finder det nødvendigt, kan den rette henvendelse til de kompetente nationale myndigheder og bede om de nærmere oplysninger, som disse er i stand til at give. Såfremt den negative udtalelse bekræftes, kan godkendelse ikke meddeles.

13. Enhver person, der er godkendt efter nr. 4 og 5, får i forbindelse med godkendelsen og herefter med jævne mellemrum de nødvendige instrukser om beskyttelsen af de klassificerede oplysninger og om, hvorledes beskyttelsen sikres. Den pågældende underskriver en erklæring som bekræftelse på, at han har modtaget disse instrukser, og at han forpligter sig til at overholde dem.

▼B

14. Ansættelsesmyndigheden træffer enhver nødvendig foranstaltning med henblik på gennemførelsen af denne afgørelse, navnlig vedrørende reglerne for adgang til listen over godkendte personer.

15. Ansættelsesmyndigheden kan undtagelsesvis og af tjenstlige grunde, forudsat den på forhånd har underrettet de kompetente myndigheder, og disse ikke har fremsat bemærkninger inden for en måned, give midlertidig godkendelse for et tidsrum, der ikke kan overstige seks måneder, medens den afventer resultatet af sikkerhedsundersøgelsen som omhandlet i nr. 7.

16. Sådanne formålsbestemte og midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET; adgang hertil er forbeholdt tjenestemænd, som har gennemgået en egentlig sikkerhedsundersøgelse med positivt resultat efter nr. 7. Indtil resultatet af sikkerhedsundersøgelsen foreligger, kan der meddeles midlertidig og formålsbestemt godkendelse til tjenestemænd, for hvem der er anmodet om sikkerhedsgodkendelse til TRÈS SECRET UE/EU TOP SECRET, så de kan få adgang til oplysninger, der er klassificeret til og med SECRET UE.

▼B

AFSNIT VII

UDARBEJDELSE, FORDELING, VIDEREGIVELSE, OPBEVARING OG DESTRUKTION AF EU-KLASSIFICERET MATERIALE

Indholdsfortegnelse

▼B

Almindelige bestemmelser

Dette afsnit indeholder nærmere bestemmelser vedrørende udarbejdelse, fordeling, videregivelse, opbevaring og destruktion af EU-klassificerede dokumenter som defineret i nr. 3, litra a), i de grundlæggende principper og minimumsstandarder for sikkerhed i del I i dette bilag. Det udgør referencerammen for tilpasning af tilsvarende foranstaltninger for andet EU-klassificeret materiale, afhængig af materialets type og fra sag til sag.

Kapitel I

Udarbejdelse og fordeling af EU-klassificerede dokumenter

UDARBEJDELSE

1. EU-klassifikationsgrader og påtegninger anvendes som omhandlet i afsnit II og anføres centreret foroven og forneden på hver side, ligesom hver side skal forsynes med nummer. Hvert dokument med EU-klassifikation skal være forsynet med referencenummer og dato. På dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET eller SECRET UE, anføres referencenummeret på hver side. Hvis dokumenter skal fordeles i flere eksemplarer, skal hvert eksemplar have et nummer, som skal anføres på første side tillige med det samlede sideantal. På dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, skal der på første side være angivet, hvor mange bilag der er.

2. Dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, må kun skrives, oversættes, opbevares, fotokopieres, reproduceres magnetisk eller mikrofilmes af personer, som er blevet sikkerhedsgodkendt med henblik på adgang til oplysninger med EU-klassifikation på et niveau, der mindst svarer til det pågældende dokuments klassifikationsgrad, bortset fra det særlige tilfælde, som er omhandlet i nr. 27 i dette afsnit.

   Bestemmelserne om anvendelse af PC m.v. til fremstilling af klassificerede dokumenter findes i afsnit XI.

FORDELING

3. EU-klassificerede oplysninger må kun komme de personer i hænde, for hvem indsigt er tjenstlig nødvendig, og som har den relevante sikkerhedsgodkendelse. Udstederen af dokumentet skal specificere, hvem der skal modtage det.

4. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, fordeles via et TRÈS SECRET UE/EU TOP SECRET-sekretariat (jf. afsnit VIII). Ved meddelelser, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, kan vedkommende sekretariat give chefen for kommunikationscentret tilladelse til at fremstille det antal kopier, som er angivet i modtagerlisten.

5. Dokumenter, der er klassificeret SECRET UE eller lavere, kan videregives af den første modtager til andre modtagere, for hvem indsigt er tjenstlig nødvendig. Udstederen skal imidlertid tydeligt angive eventuelle nærmere betingelser. Angives sådanne nærmere betingelser, må modtagerne kun videregive dokumentet med udstederens samtykke.

6. Ethvert dokument, der er klassificeret CONFIDENTIEL UE eller højere, registreres ved såvel modtagelse og som udsendelse af sekretariatet i den instans, som modtager eller udsender det. De oplysninger (dokumentreference, dato og evt. eksemplarnummer), som er nødvendige for at kunne identificere dokumentet, indføres i en journal eller i en særligt beskyttet edb-databærer.

Kapitel II

Videregivelse af EU-klassificerede dokumenter

KUVERTER

7. Dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, sendes i to uigennemsigtige kuverter af svært papir. Den inderste kuvert forsynes med angivelse af den pågældende EU-klassifikationsgrad og om muligt udførlig angivelse af modtagerens stilling og kontoradresse.

8. Kun sekretariatets leder eller dennes stedfortræder må åbne den inderste kuvert og kvittere for modtagelsen af dokumenterne, medmindre kuverten er adresseret til en bestemt person. I så fald journaliseres kuverten af det pågældende sekretariat, og kun den person, den er adresseret til, må åbne den inderste kuvert og kvittere for modtagelsen af de fremsendte dokumenter.

▼B

9. Den inderste kuvert skal indeholde en kvitteringsformular. Kvitteringen, som ikke er klassificeret, skal indeholde oplysning om dokumentreference, dato og eksemplarnummer, men aldrig om, hvad sagen vedrører.

10. Den inderste kuvert anbringes i en kuvert, som forsynes med et registreringsnummer. Klassifikationsgraden må under ingen omstændigheder angives på den yderste kuvert.

11. Ved dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, modtager kureren en kvittering for hvert registreringsnummer.

TRANSPORT INDEN FOR EN BYGNING ELLER GRUPPE AF BYGNINGER

12. Inden for en given bygning eller gruppe af bygninger kan klassificerede dokumenter bæres i en forseglet kuvert, som kun er forsynet med modtagerens navn, når blot den person, der bærer dem, er sikkerhedsgodkendt til de pågældende dokumenters klassifikationsgrad.

VIDEREGIVELSE AF EU-DOKUMENTER INDEN FOR ET LANDS GRÆNSER

13. Inden for et lands grænser sendes dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, kun med officiel kurertjeneste eller med personer, der er sikkerhedsgodkendt til TRÈS SECRET UE/EU TOP SECRET.

14. Hvis dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, sendes med kurertjeneste uden for en bygning eller gruppe af bygninger, skal bestemmelserne om emballering og modtagelse i dette kapitel altid overholdes. Kurertjenesternes bemanding skal være tilstrækkelig til, at pakker indeholdende dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, til enhver tid er under direkte opsyn af en ansvarlig medarbejder.

15. Undtagelsesvis kan et dokument, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, medbringes til lokalt brug ved møder og drøftelser af andre medarbejdere end kurerer uden for en bygning eller gruppe af bygninger, men kun på følgende betingelser:

    a) bæreren af dokumentet skal være sikkerhedsgodkendt til og være berettiget til indsigt i TRÈS SECRET UE/EU TOP SECRET-dokumenter

    b) transportmåden skal være i overensstemmelse med landets regler om forsendelse af nationale YDERST HEMMELIGT-dokumenter

    c) den pågældende må under ingen omstændigheder efterlade dokumentet, der er klassificeret TRÈS SECRET UE/EU TOP SECRET uden opsyn

    d) en fortegnelse over dokumenter, der transporteres på denne måde, opbevares i TRÈS SECRET UE/EU TOP SECRET-sekretariatet, som har ansvaret for dokumenterne, og indføres i en journal, og dokumenterne sammenholdes med denne fortegnelse, når de leveres tilbage.

16. Inden for et givet lands grænser kan dokumenter, der er klassificeret SECRET UE eller CONFIDENTIEL UE, sendes med posten, hvis dette er tilladt efter landets egne bestemmelser og er i overensstemmelse med disse bestemmelser, eller de kan sendes med kurertjeneste eller med personer, der er sikkerhedsgodkendt til at få indsigt i EU-klassificerede oplysninger.

17. Hver medlemsstat og hvert decentralt EU-organ udarbejder på grundlag af disse bestemmelser instrukser om personlig transport af EU-klassificerede dokumenter. Den, der bærer sådanne dokumenter, skal læse og underskrive disse instrukser. Det skal navnlig fremgå klart af instrukserne, at dokumenterne under ingen omstændigheder må:

    a) overlades til andre, medmindre de deponeres i overensstemmelse med bestemmelserne i afsnit IV

    b) efterlades uden opsyn i offentlige transportmidler eller private køretøjer eller på steder som restauranter eller hoteller. De må ikke opbevares i hotelbokse eller efterlades uden opsyn på hotelværelser

    c) læses på offentlige steder såsom i fly eller tog.

VIDEREGIVELSE FRA EN MEDLEMSSTAT TIL EN ANDEN

18. Materiale, der er klassificeret CONFIDENTIEL UE eller højere, sendes fra en medlemsstat til en anden med diplomatpost eller militær kurertjeneste.

19. Der kan imidlertid gives tilladelse til personlig transport af materiale, der er klassificeret SECRET UE eller CONFIDENTIEL UE, hvis det kan sikres, at materialet transporteres på en sådan måde, at det ikke kan komme uautoriserede personer i hænde.

▼B

20. De nationale sikkerhedsmyndigheder kan give tilladelse til personlig transport, hvis der ikke er mulighed for diplomatpost eller en militær kurer, eller hvis anvendelse heraf vil medføre en forsinkelse, der vil skade EU's operationer, og det haster at få materialet frem til modtageren. Hver medlemsstat udarbejder instrukser om anden form for personlig transport end diplomatpost og militær kurertjeneste med henblik på international forsendelse af materiale med klassifikationsgrad til og med SECRET UE. Instrukserne skal indeholde følgende krav:

    a) den, der bærer materialet, skal have medlemsstaternes relevante sikkerhedsgodkendelse

    b) alt, hvad der transporteres på denne måde, skal registreres af vedkommende sekretariat

    c) pakker og bagage, mv., der indeholder EU-klassificeret materiale, skal plomberes officielt for at undgå toldeftersyn og skal mærkes med identifikation og instrukser til finderen

    d) den pågældende skal være i besiddelse af et kurercertifikat og/eller en tjenesterejseordre, som anerkendes af alle EU-medlemsstater og giver tilladelse til at transportere pakken som beskrevet

    e) den pågældende må ikke ved rejse over land rejse gennem en stat, som ikke er medlem af EU, eller krydse dens grænse, medmindre den stat, der står for transporten, er i besiddelse af en særlig garanti fra denne stat

    f) den pågældendes rejseplaner med hensyn til bestemmelsessted, rejseruter og anvendte transportmidler skal være i overensstemmelse med EU-bestemmelserne eller med de nationale bestemmelser herom, hvis disse er strengere end EU's

    g) materialet skal hele tiden være i den pågældendes varetægt, medmindre det deponeres i overensstemmelse med bestemmelserne om deponering i afsnit IV

    h) materialet må ikke efterlades uden opsyn i offentlige eller private køretøjer eller på steder som restauranter eller hoteller. Det må ikke opbevares i hotelbokse eller efterlades uden opsyn på hotelværelser

    i) hvis det transporterede materiale omfatter dokumenter, må disse ikke læses på offentlige steder (f.eks. i fly eller tog).

    Den person, der udpeges til at transportere det klassificerede materiale, skal læse og underskrive en sikkerhedsorientering, der som et minimum omfatter ovennævnte instrukser samt de procedurer, der skal følges i en krisesituation eller i tilfælde af, at pakken med det klassificerede materiale kræves undersøgt af toldmyndighederne eller sikkerhedspersonalet i en lufthavn.

VIDEREGIVELSE AF DOKUMENTER, DER ER KLASSIFICERET RESTREINT UE

21. Der fastsættes ingen særlige bestemmelser for forsendelse af dokumenter, der er klassificeret RESTREINT UE; det skal dog sikres, at uvedkommende ikke kommer i besiddelse af dem.

SIKKERHEDSGODKENDELSE AF KURERPERSONALE

22. Alle kurerer, der ansættes til at transportere dokumenter, der er klassificeret SECRET UE og CONFIDENTIEL UE, skal forinden have den relevante sikkerhedsgodkendelse.

Kapitel III

Elektronisk eller anden teknisk videregivelse

23. Der træffes foranstaltninger med hensyn til kommunikationssikkerhed, så EU-klassificerede oplysninger kan videregives under sikre forhold. De nærmere bestemmelser om sådan videregivelse af EU-klassificerede oplysninger er omhandlet i afsnit XI.

24. Oplysninger, der er klassificeret CONFIDENTIEL UE eller SECRET UE, må kun videregives via godkendte kommunikationscentre og -netværk og/eller godkendte terminaler og systemer.

Kapitel IV

Kopiering, oversættelse og uddrag af EU-klassificerede dokumenter

25. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, må kun kopieres eller oversættes med udstederens godkendelse.

▼B

26. Hvis medarbejdere, der ikke er sikkerhedsgodkendt til TRÈS SECRET UE/EU TOP SECRET har brug for oplysninger, som er indeholdt i et TRÈS SECRET UE/EU TOP SECRET-dokument, men ikke er klassificeret så højt, kan lederen af TRÈS SECRET UE/EU TOP SECRET-sekretariatet opnå tilladelse til at udlevere de nødvendige uddrag af det pågældende dokument. Vedkommende tager samtidig de nødvendige skridt til at sikre, at uddragene klassificeres på et passende niveau.

27. Dokumenter, der er klassificeret SECRET UE eller lavere, kan mangfoldiggøres og oversættes af modtageren inden for rammerne af de nationale sikkerhedsbestemmelser, for så vidt det sker under nøje overholdelse af »need-to-know«-princippet. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, skal også gælde for kopier og/eller oversættelser af det. Decentrale EU-organer følger disse sikkerhedsforskrifter.

Kapitel V

Fornyet gennemgang og kontrol, opbevaring og destruktion af EU-klassificerede dokumenter

FORNYET GENNEMGANG OG KONTROL

28. Hvert år gennemgår det i afsnit VIII omhandlede TRÈS SECRET UE/EU TOP SECRET-sekretariat hvert af de dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, i overensstemmelse med bestemmelserne i afsnit VIII, nr. 9-11. Der foretages intern kontrol af EU-klassificerede dokumenter, der er klassificeret lavere end TRÈS SECRET UE/EU TOP SECRET, i overensstemmelse med nationale retningslinjer, og for så vidt angår GSR og decentrale EU-organer, i overensstemmelse med instrukser fra generalsekretæren/den højtstående repræsentant.

    En sådan fornyet gennemgang og kontrol giver mulighed for at indhente ihændehavernes opfattelse af, hvilke dokumenter der kan:

    a) nedklassificeres eller afklassificeres

    b) destrueres.

ARKIVERING AF EU-KLASSIFICEREDE OPLYSNINGER

29. For at begrænse opbevaringsproblemerne mest muligt har sekretariatets leder bemyndigelse til at lade dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE, mikrofilme eller på anden måde arkivere i en magnetisk eller optisk udgave på følgende betingelser:

    a) optagelsen på mikrofilm/arkiveringen skal foretages af personale, der har en gyldig sikkerhedsgodkendelse svarende til det enkelte dokuments klassifikationsgrad

    b) der gælder samme sikkerhedsbestemmelser for det medium, der anvendes til optagelsen/arkiveringen, som for de oprindelige dokumenter

    c) udstederen underrettes om optagelse/arkivering af dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET

    d) filmruller eller andre former for medier må kun indeholde dokumenter med samme klassifikationsgrad, dvs. enten TRÈS SECRET UE/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE

    e) optagelse/arkivering af et dokument, der er klassificeret TRÈS SECRET UE/EU TOP SECRET eller SECRET UE, angives tydeligt i den journal, der anvendes til den årlige oversigt

    f) originale dokumenter, som er blevet mikrofilmet, eller som opbevares på anden vis, tilintetgøres i overensstemmelse med bestemmelserne i nr. 28-32 nedenfor.

30. Disse bestemmelser gælder ligeledes for enhver anden form for opbevaring, som godkendes af den nationale sikkerhedsmyndighed, såsom elektromagnetiske og optiske medier.

RUTINEMÆSSIG DESTRUKTION AF EU-KLASSIFICEREDE DOKUMENTER

31. For at undgå unødvendig ophobning af EU-klassificerede dokumenter destrueres dokumenter, som chefen for den instans, styrelse m.v., hvor de opbevares, anser for at være forældede eller overskydende, så hurtigt som muligt på følgende måde:

    a) dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, må kun destrueres af det sekretariat, som er ansvarligt for dem. Hvert af de destruerede dokumenter anføres i en erklæring om destruktionen, som

▼B

underskrives af den sikkerhedsansvarlige på TRÈS SECRET UE/EU TOP SECRET-niveau og af den medarbejder, der overværer destruktionen, og som skal være sikkerhedsgodkendt til TRÈS SECRET UE/EU TOP SECRET. Der indføres en bemærkning herom i journalen

b) erklæringer om destruktion samt fortegnelser over fordeling opbevares af sekretariatet i ti år. Der skal kun sendes kopier til udstederen eller det relevante centrale sekretariat på udtrykkelig anmodning

c) dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og karbonpapir, destrueres under opsyn af en ansvarlig på TRÈS SECRET UE/EU TOP SECRET-niveau ved afbrænding, opløsning, makulering eller på anden måde reducering til et produkt, der hverken kan genkendes eller rekonstrueres.

32. Dokumenter, der er klassificeret SECRET UE, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, under opsyn af en sikkerhedsgodkendt medarbejder og ved hjælp af processerne i nr. 31, litra c). Destruerede dokumenter, der var klassificeret SECRET UE, anføres på underskrevne erklæringer om destruktion, som opbevares af sekretariatet i mindst tre år tillige med fortegnelser over udbredelse.

33. Dokumenter, der er klassificeret CONFIDENTIEL UE, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, under opsyn af en sikkerhedsgodkendt medarbejder og ved hjælp af processerne i nr. 31, litra c). Destruktionen registreres i overensstemmelse med nationale bestemmelser eller, hvis det drejer sig om GSR eller decentrale EU-organer, efter instrukser fra generalsekretæren/den højtstående repræsentant.

34. Dokumenter, der er klassificeret RESTREINT UE, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, eller af brugeren i overensstemmelse med nationale bestemmelser eller, hvis det drejer sig om GSR eller decentrale EU-organer, efter instruks fra generalsekretæren/den højtstående repræsentant.

DESTRUKTION I KRISESITUATIONER

35. GSR, medlemsstaterne og de decentrale EU-organer udarbejder på grundlag af lokale forhold planer for sikker opbevaring af EU-klassificeret materiale i krisesituationer, herunder om nødvendigt planer for destruktion eller flytning; de bekendtgør i deres respektive instanser de instrukser, som de finder nødvendige for at undgå, at uautoriserede personer får EU-klassificerede oplysninger i hænde.

36. Foranstaltningerne til sikker opbevaring og/eller destruktion i krisesituationer af materiale, der er klassificeret SECRET UE eller CONFIDENTIEL UE, må under ingen omstændigheder være til skade for opbevaringen eller destruktionen af materiale, der er klassificeret TRÈS SECRET UE/EU TOP SECRET; dette gælder ligeledes krypteringsudstyr, som skal prioriteres over alt andet. Der udstedes ad hoc-instrukser vedrørende foranstaltninger til sikker opbevaring og tilintetgørelse af krypteringsudstyr i en krisesituation.

Kapitel VI

Særlige bestemmelser for dokumenter til brug i Rådet

37. Inden for GSR fører Sekretariatet for Klassificerede Oplysninger (B.I.C.) kontrol med de oplysninger, der er klassificeret SECRET UE eller CONFIDENTIEL UE, hvis disse oplysninger indgår i dokumenter til brug i Rådet.

Med reference til generaldirektøren for personale og administration har dette sekretariat til opgave

a) at administrere opgaverne vedrørende oplysningernes journalisering, gengivelse, oversættelse, forsendelse, transport og tilintetgørelse

b) at ajourføre listen med data vedrørende klassificerede oplysninger

c) med regelmæssige mellemrum at spørge udstederne om, hvorvidt det er nødvendigt at opretholde klassifikationen af oplysningerne

d) i samråd med Sikkerhedskontoret at fastsætte de nærmere praktiske bestemmelser for klassificering og afklassificering af oplysninger.

38. Sekretariatet for Klassificerede Oplysninger (B.I.C.) fører et register, der omfatter følgende data:

a) dato for udfærdigelsen af den klassificerede oplysning

b) klassifikationsgrad

▼B

c) den dato, indtil hvilken oplysningen er klassificeret

d) udstederens navn og tjenestegren

e) modtageren eller modtagerne med angivelse af løbenummer

f) emne

g) nummer

h) antal videregivne eksemplarer

i) opgørelser over, hvilke klassificerede oplysninger der er forelagt Rådet

j) registrering af afklassificering og nedklassificering af klassificerede oplysninger.

39. De almindelige bestemmelser i kapitel I-V i dette afsnit gælder for Sekretariatet for Klassificerede Oplysninger (B.I.C.), medmindre de særlige bestemmelser i dette kapitel afviger herfra.

▼B

AFSNIT VIII

TRÈS SECRET UE/EU TOP SECRET-SEKRETARIATER

1. Formålet med TRÈS SECRET UE/EU TOP SECRET-sekretariaterne er at sikre, at dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, journaliseres, behandles og fordeles i overensstemmelse med sikkerhedsbestemmelserne. Lederen af TRÈS SECRET UE/EU TOP SECRET-sekretariatet i henholdsvis den enkelte medlemsstat, GSR eller decentrale EU-organer er den sikkerhedsansvarlige for klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET.

2. Det centrale sekretariat er hovedkontoret for modtagelse og afsendelse både i medlemsstaterne, i GSR og i de af de decentrale EU-organer, hvor der er oprettet et sådant kontor, samt eventuelt i andre EU-institutioner, internationale organisationer og tredjelande, med hvilke Rådet har indgået aftaler om sikkerhedsprocedurer for udveksling af klassificerede oplysninger.

3. Om nødvendigt oprettes der undersekretariater med ansvar for den interne styring af dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET; undersekretariaterne registrerer løbende, hvor samtlige dokumenter, som de er ansvarlige for, befinder sig.

4. Hvis der er et langsigtet behov herfor, oprettes der efter retningslinjerne i afsnit I TRÈS SECRET UE/EU TOP SECRET-undersekretariater, som knyttes til det centrale TRÈS SECRET UE/EU TOP SECRET-sekretariat. Hvis der kun midlertidigt og lejlighedsvis er behov for at konsultere dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, kan sådanne dokumenter fordeles uden oprettelse af et TRÈS SECRET UE/EU TOP SECRET-undersekretariat, men der skal fastsættes regler, der sikrer, at det pågældende TRÈS SECRET UE/EU TOP SECRET-sekretariat stadig har kontrol med dokumenterne, og at samtlige fysiske og personalemæssige sikkerhedsforanstaltninger overholdes.

5. Undersekretariaterne må ikke sende dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, direkte til andre undersekretariater under samme centrale TRÈS SECRET UE/EU TOP SECRET-sekretariat uden sidstnævntes udtrykkelige godkendelse.

6. Al udveksling af dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, mellem undersekretariater, som ikke er knyttet til samme centrale sekretariat, skal foregå via det centrale TRÈS SECRET UE/EU TOP SECRET-sekretariat.

DET CENTRALE TRÈS SECRET UE/EU TOP SECRET-SEKRETARIAT

7. Som sikkerhedsansvarlig er lederen af det centrale TRÈS SECRET UE/EU TOP SECRET-sekretariat ansvarlig for:

   a) at dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, forsendes i overensstemmelse med bestemmelserne i afsnit VII

   b) at en fortegnelse over samtlige TRÈS SECRET UE/EU TOP SECRET-undersekretariater, der er knyttet til det pågældende centrale sekretariat, samt en liste med de udpegede sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift til stadighed holdes ajour

   c) at arkivkvitteringer for alle TRÈS SECRET UE/EU TOP SECRET-dokumenter, som fordeles via det centrale sekretariat, opbevares

   d) at opbevarede og fordelte TRÈS SECRET UE/EU TOP SECRET-dokumenter journaliseres

   e) at en fortegnelse over alle de centrale TRÈS SECRET UE/EU TOP SECRET-sekretariater, som vedkommende jævnligt er i forbindelse med, tillige med de udpegede sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift løbende holdes ajour

   f) at alle sekretariatets dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, sikres fysisk i overensstemmelse med bestemmelserne i afsnit IV.

TRÈS SECRET UE/EU TOP SECRET-UNDERSEKRETARIATER

8. Som sikkerhedsansvarlig er lederen af et TRÈS SECRET UE/EU TOP SECRET-undersekretariat ansvarlig for:

   a) at dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, forsendes i overensstemmelse med bestemmelserne i afsnit VII og nr. 5-6 i afsnit VIII

▼B

b) at en fortegnelse over alle, der har adgang til de TRÈS SECRET UE/EU TOP SECRET-klassificerede oplysninger, der er i vedkommendes varetægt løbende holdes ajour

c) at dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, fordeles i overensstemmelse med udstederens instrukser eller efter »need-to-know«-princippet, såfremt det kan fastslås, at modtageren har den fornødne sikkerhedsgodkendelse

d) at alle dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, og hvis opbevaring og fordeling sker under vedkommendes kontrol, eller som er overført til andre TRÈS SECRET UE/EU TOP SECRET-sekretariater, løbende journaliseres, og at samtlige kvitteringer i forbindelse hermed opbevares

e) at en fortegnelse over de TRÈS SECRET UE/EU TOP SECRET-sekretariater, som vedkommende har bemyndigelse til at udveksle TRÈS SECRET UE/EU TOP SECRET-dokumenter med, tillige med de sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift løbende holdes ajour

f) at alle undersekretariatets dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, sikres fysisk i overensstemmelse med bestemmelserne i afsnit IV.

ÅRSOPGØRELSE

9. Hver tolvte måned udarbejder hvert TRÈS SECRET UE/EU TOP SECRET-sekretariat en specificeret opgørelse over alle de TRÈS SECRET UE/EU TOP SECRET-dokumenter, som det er ansvarligt for. Sekretariatet anses for at have redegjort for et dokument, hvis det fysisk er i besiddelse af dokumentet eller af en kvittering fra det TRÈS SECRET UE/EU TOP SECRET-sekretariat, hvortil dokumentet er blevet sendt, en erklæring om tilintetgørelse af det pågældende dokument eller en instruks om at nedklassificere eller afklassificere det.

10. Undersekretariaterne sender resultatet af deres årsopgørelse til det centrale sekretariat, som de har reference til, på en dato, som fastsættes af det centrale sekretariat.

11. De nationale sikkerhedsmyndigheder samt de EU-institutioner, internationale organisationer og decentrale EU-organer, hvor der findes et TRÈS SECRET UE/EU TOP SECRET-sekretariat, sender hvert år senest den 1. april resultatet af årsopgørelserne i de centrale TRÈS SECRET UE/EU TOP SECRET-sekretariater til generalsekretæren/den højtstående repræsentant.

▼B

AFSNIT IX

SIKKERHEDSFORANSTALTNINGER, HVIS DER VED MØDER UDEN FOR RÅDETS BYGNINGER SKAL BEHANDLES MEGET FØLSOMME SPØRGSMÅL

ALMINDELIGE BESTEMMELSER

1. Hvis møder i Det Europæiske Råd eller Rådet, ministermøder eller andre vigtige møder ikke afholdes i Rådets lokaler i Bruxelles eller Luxembourg, og hvis særlige sikkerhedshensyn kræver det, fordi der på sådanne møder skal behandles meget følsomme spørgsmål eller oplysninger, træffes nedenstående sikkerhedsforanstaltninger. Disse foranstaltninger vedrører udelukkende beskyttelse af EU-klassificerede oplysninger; det kan være nødvendigt at træffe yderligere sikkerhedsforanstaltninger.

ANSVARSFORDELING

Værtslandet

2. Den medlemsstat, på hvis område sådanne møder afholdes (værtslandet), er i samarbejde med GSR's Sikkerhedskontor ansvarlig for sikkerheden i forbindelse med møder i Det Europæiske Råd eller Rådet, ministermøder eller andre vigtige møder samt for de ledende delegeredes og disses medarbejderes fysiske sikkerhed.

   Dette krav om sikkerhedsbeskyttelse indebærer, at:

   a) der udarbejdes planer for håndtering af sikkerhedstrusler og sikkerhedsrelaterede hændelser, og at de relevante foranstaltninger navnlig tager sigte på at opbevare EU-klassificerede dokumenter på kontorerne under sikre forhold

   b) der træffes foranstaltninger til at give adgang til Rådets kommunikationssystem med henblik på modtagelse og videregivelse af EU-klassificerede oplysninger. Værtslandet stiller i nødvendigt omfang sikrede telefonsystemer til rådighed.

Medlemsstaterne

3. Myndighederne i medlemsstaterne tager de nødvendige skridt til at sikre, at:

   a) attestation af relevant sikkerhedsgodkendelse af deres egne delegerede sendes enten direkte til den sikkerhedsansvarlige for møderne eller via GSR's Sikkerhedskontor, om nødvendigt elektronisk eller med fax

   b) værtslandets myndigheder og i givet fald GSR's Sikkerhedskontor underrettes om enhver konkret trussel, så der kan træffes passende foranstaltninger.

Sikkerhedsofficeren for møderne

4. Der udpeges en sikkerhedsofficer, som har ansvar for det almindelige forberedende arbejde, for at kontrollere de almindelige interne sikkerhedsforanstaltninger og for at koordinere samarbejdet med andre involverede sikkerhedsmyndigheder. Vedkommende sørger navnlig for:

   a) i) beskyttelse af mødelokaliteterne, så det sikres, at mødet kan afholdes uden hændelser, der kunne indebære en sikkerhedsrisiko for eventuelle EU-klassificerede oplysninger, som skal behandles på mødet

      ii) kontrol af de personer, som har adgang til mødelokaliteterne, delegationernes lokaler og mødelokaler, samt kontrol af alt udstyr

      iii) løbende samordning med værtslandets kompetente myndigheder og GSR's Sikkerhedskontor

   b) indsættelse af et eksemplar af sikkerhedsinstrukserne i hvert dokumentcharteque til mødet under hensyn til de krav, der er indeholdt i sikkerhedsforskrifter, og til alle andre sikkerhedsinstrukser, som måtte findes relevante.

GSR's Sikkerhedskontor

5. GSR's Sikkerhedskontor fungerer som sikkerhedsrådgiver under forberedelsen af møderne; det sender en repræsentant til stedet til at assistere og rådgive sikkerhedsofficeren for mødet og delegationerne.

6. Hver af delegationerne udpeger en sikkerhedsofficer, som har ansvaret for sikkerhedsspørgsmål i den pågældende delegation og for at opretholde den fornødne kontakt med sikkerhedsofficeren for møderne og med GSR's Sikkerhedskontor.

▼B

SIKKERHEDSFORANSTALTNINGER

Sikkerhedszoner

7. Der oprettes følgende sikkerhedszoner:

   a) sikkerhedszone af klasse II, bestående af arbejdsrum, GSR-kontorer og reprografisk udstyr samt delegationskontorer, hvis dette er relevant

   b) sikkerhedszone af klasse I, bestående af mødelokalet med bokse til tolke og lydteknikere

   c) administrative zoner, bestående af presselokalerne og de dele af mødelokaliteterne, som anvendes til administrativt arbejde, forplejning og indkvartering samt det område, der støder op til pressecentret og mødelokaliteterne.

Adgangsbadger

8. Sikkerhedsofficeren for mødet udsteder de adgangsbadger, delegationerne har bedt om. Om nødvendigt kan der sondres mellem adgang til de enkelte sikkerhedszoner.

9. Det bør fremhæves i sikkerhedsinstrukserne, at alle involverede konstant skal bære deres adgangsbadge, så det tydeligt kan ses, så længe de befinder sig i mødelokaliteterne, så sikkerhedspersonalet kan foretage den nødvendige kontrol.

10. Ud over deltagere med adgangsbadge skal så få som muligt have adgang til mødelokaliteterne. Hvis de enkelte landes delegationer ønsker at modtage besøg under mødet, underretter de sikkerhedsofficeren for mødet herom. Besøgende får udleveret et gæstekort. Der udfyldes en formular med den besøgendes navn og navnet på den person, som den besøgende skal møde. Besøgende ledsages til stadighed af en sikkerhedsvagt eller af den person, som den besøgende skal møde. Ovennævnte formular medbringes af den person, der ledsager den besøgende, og leveres tilbage til sikkerhedspersonalet sammen med gæstebadgen, når den besøgende forlader mødelokaliteterne.

Kontrol af foto- og andet optageudstyr

11. Der må ikke bringes kameraer eller udstyr til lydoptagelser ind i en sikkerhedszone af klasse I; dog er udstyr, som medbringes af fotografer og lydteknikere med tilladelse fra den sikkerhedsansvarlige for mødet, undtaget herfra.

Undersøgelse af dokumentmapper, bærbare computere og pakker

12. Personer med adgangsbadge til en sikkerhedszone må normalt medbringe deres dokumentmapper og bærbare computere (må ikke tilsluttes lysnettet), uden at disse undersøges. Sendes der pakker til delegationerne, må disse modtage pakkerne, som enten undersøges af delegationens sikkerhedsofficer, gennemlyses med særligt udstyr eller åbnes af sikkerhedspersonalet med henblik på nærmere undersøgelse. Hvis sikkerhedsofficeren for mødet finder det nødvendigt, kan der træffes skærpede kontrolforanstaltninger for undersøgelse af dokumentmapper og pakker.

Teknisk sikkerhed

13. Mødelokalet kan sikres teknisk af tekniske sikkerhedseksperter, som også kan foretage elektronisk overvågning under mødet.

Dokumenter i delegationernes varetægt

14. Delegationerne er ansvarlige for at transportere EU-klassificerede dokumenter til og fra møderne. De er ligeledes ansvarlige for kontrol og sikkerhed, når sådanne dokumenter anvendes i de dertil indrettede lokaler. De kan anmode om assistance fra værtslandet til transport af klassificerede dokumenter til og fra mødelokaliteterne.

Sikker opbevaring af dokumenter

15. Hvis GSR, Kommissionen eller delegationerne ikke er i stand til at opbevare deres klassificerede dokumenter i overensstemmelse med godkendte normer, kan de mod kvittering deponere dokumenterne i en forseglet kuvert hos sikkerhedsofficeren for mødet, som derefter opbevarer dokumenterne i overensstemmelse med godkendte normer.

Kontoreftersyn

16. Sikkerhedsofficeren for mødet drager omsorg for, at GSR's og delegationernes kontorer efterses efter hver arbejdsdag for at sikre, at samtlige EU-klassificerede dokumenter opbevares på et sikkert sted; hvis han finder, at dette ikke er tilfældet, træffer han de fornødne foranstaltninger.

▼B

Bortskaffelse af EU-klassificeret affald

17. Alt affald behandles som EU-klassificeret, og papirkurve og affaldsposer afleveres til GSR og delegationerne med henblik på bortskaffelse. Inden GSR og delegationerne forlader de lokaler, som er blevet dem tildelt, afleverer de deres affald til sikkerhedsofficeren for mødet, som sørger for, at det destrueres efter gældende bestemmelser.

18. Ved mødets afslutning behandles samtlige dokumenter, som GSR eller delegationerne er i besiddelse af, men ikke længere har brug for, som affald. Der foretages en grundig gennemsøgning af de lokaler, som GSR og delegationerne har anvendt, inden sikkerhedsforanstaltningerne for mødet ophæves. Dokumenter, for hvilke der er kvitteret ved underskrift, destrueres så vidt muligt som foreskrevet i afsnit VII.

▼B

AFSNIT X

BRUD PÅ SIKKERHEDSBESTEMMELSERNE OG RISIKO FOR LÆKAGE AF EU-KLASSIFICEREDE OPLYSNINGER

1. Et brud på sikkerhedsbestemmelserne er en handling eller forsømmelse, hvorved Rådets eller de nationale sikkerhedsbestemmelser overtrædes, og EU-klassificerede oplysninger ikke længere er sikrede og risikerer at lække.

2. EU-klassificerede oplysninger anses for at være lækket, enten hvis de helt eller delvist kommer uautoriserede personer i hænde, som hverken har den nødvendige sikkerhedsgodkendelse, eller for hvem indsigt ikke er tjenstlig nødvendig, eller hvis det må anses for sandsynligt, at en sådan hændelse er indtruffet.

3. EU-klassificerede oplysninger kan lække som følge af skødesløse eller uagtsomme handlinger eller uoverlagte ytringer, samt hvis EU og dets medlemsstater, for så vidt angår EU-klassificerede oplysninger eller aktiviteter gøres til genstand for spionage eller undergravende virksomhed.

4. Det er vigtigt, at enhver, der pålægges at behandle EU-klassificerede oplysninger, grundigt orienteres om sikkerhedsprocedurerne og risikoen ved uoverlagte ytringer, navnlig over for pressen. Det bør indskærpes, at det er vigtigt straks at rapportere om ethvert brud på sikkerheden, man måtte blive opmærksom på, til vedkommende sikkerhedsmyndighed i medlemsstaten, institutionen eller det decentrale organ.

5. Opdager en sikkerhedsmyndighed, at der er sket et brud på sikkerhedsbeskyttelsen af EU-klassificerede oplysninger, eller at EU-klassificerede oplysninger er gået tabt eller forsvundet, eller underrettes den om en sådan hændelse, skal den træffe de fornødne foranstaltninger for at

   a) fastslå omstændighederne

   b) vurdere og begrænse den forvoldte skade

   c) forebygge en gentagelse

   d) underrette vedkommende myndigheder om følgerne af det brud, der er sket på sikkerhedsbeskyttelsen.

   I den forbindelse skal følgende oplysninger meddeles:

   i) i en beskrivelse af arten af de pågældende klassificerede oplysninger, herunder klassifikationsgrad, dokument- og eksemplarnummer, dato, udsteder, emne og sagsområde

   ii) en kort beskrivelse af omstændighederne for bruddet på sikkerhedsbestemmelserne, herunder dato, samt angivelse af hvor længe de pågældende oplysninger ikke har været beskyttede

   iii) en erklæring om, hvorvidt udstederen er blevet underrettet.

6. Hver sikkerhedsmyndighed har pligt til, så snart den får meddelelse om, at der er sket et brud på sikkerheden, øjeblikkeligt at rapportere forholdet under anvendelse af følgende procedure: TRÈS SECRET UE/EU TOP SECRET-undersekretariater rapporterer hændelsen til Sikkerhedskontoret i GSR via vedkommende centrale TRÈS SECRET UE/EU TOP SECRET-sekretariat; såfremt EU-klassificerede oplysninger lækker inden for en medlemsstats jurisdiktion, rapporteres hændelsen til sikkerhedskontoret i GSR, som specificeret i punkt 5, via vedkommende nationale sikkerhedsmyndigheder.

7. Vedrører hændelsen oplysninger, der er klassificeret RESTREINT UE, rapporteres kun, hvis der foreligger usædvanlige omstændigheder.

8. Generalsekretæren/den højtstående repræsentant skal, når han bliver orienteret om, at der er sket et brud på sikkerheden:

   a) underrette den myndighed, der har udstedt de pågældende klassificerede oplysninger

   b) anmode de relevante sikkerhedsmyndigheder om at iværksætte undersøgelser

   c) samordne undersøgelser, hvor mere end en sikkerhedsmyndighed er involveret

   d) modtage en rapport om omstændighederne for bruddet, datoen samt angivelse af, hvor længe de pågældende oplysninger ikke har været beskyttede, hvordan det blev opdaget, samt de pågældende oplysningers emne og klassifikationsgrad. Den skade, der er forvoldt EU's eller en eller flere af medlemsstaternes interesser, samt de foranstaltninger, der er truffet for at forebygge gentagelser, skal ligeledes rapporteres.

▼B

9. Den myndighed, der har udstedt de pågældende oplysninger, orienterer modtagerne og meddeler, hvordan de skal forholde sig.

10. Enhver, der har ansvaret for lækage af EU-klassificerede oplysninger, pålægges disciplinære sanktioner i henhold til de relevante regler og bestemmelser. Disciplinære sanktioner udelukker ikke, at den ansvarlige ligeledes retsforfølges.

▼B

AFSNIT XI

BESKYTTELSE AF OPLYSNINGER, DER BEHANDLES I INFORMATIONSTEKNOLOGI- OG KOMMUNIKATIONSSYSTEMER

Indholdsfortegnelse

▼B

Kapitel I

Indledning

GENERELLE ASPEKTER

1. Sikkerhedspolitikken og -kravene i dette afsnit gælder for alle kommunikations- og informationssystemer og net (i det følgende benævnt »SYSTEMER«), som behandler oplysninger, der er klassificeret CONFIDENTIEL UE eller højere.

2. SYSTEMER, som behandler oplysninger, der er klassificeret RESTREINT UE, kræver ligeledes sikkerhedsforanstaltninger. Alle SYSTEMER kræver sikkerhedsforanstaltninger til at beskytte de oplysninger, de indeholder, mod uautoriseret ændring og sikre, at de er til rådighed, når de skal anvendes. De sikkerhedsforanstaltninger, der skal anvendes på sådanne systemer, vil blive fastlagt af den udpegede godkendelsesmyndighed under hensyn til den vurderede risiko og i overensstemmelse med den politik, der er formuleret i disse sikkerhedsforskrifter.

3. Beskyttelse af sensorsystemer, der indeholder informationsteknologisystemer, bestemmes og specificeres generelt i de systemer, de tilhører, ved anvendelse af bestemmelserne i dette afsnit i det omfang, det er muligt.

TRUSLER MOD SYSTEMER OG DERES SÅRBARHED

4. Generelt kan trussel defineres som sandsynligheden for uagtsom eller bevidst lækage af oplysninger. I forbindelse med SYSTEMER indebærer lækage, at en eller flere sikkerhedsfeatures, der skal beskytte klassificerede oplysninger mod uautoriseret ændring og sikre, at de er til rådighed, når de skal anvendes. Sårbarhed kan defineres som en svaghed eller utilstrækkelig kontrol, som vil lette eller tillade, at en trussel aktiveres mod et specifikt aktiv eller mål. En sårbarhed kan være en tjenstlig forsømmelse eller kan vedrøre et svagt led i en kontrols effektivitet, omfang eller konsekvens og kan være teknisk, proceduremæssig eller operationel.

5. Både EU-klassificerede og uklassificerede oplysninger, der behandles i SYSTEMER i komprimeret form med henblik på hurtig søgning, datatransmission og udnyttelse, er udsat for mange risici. Uautoriserede kan få adgang til oplysningerne, eller autoriserede kan blive nægtet adgang. Der er ligeledes risiko for uautoriseret offentliggørelse, forvanskning, ændring eller sletning af oplysningerne. Endvidere er det komplekse og undertiden skrøbelige udstyr kostbart og ofte vanskeligt at reparere eller udskifte hurtigt. Disse SYSTEMER er derfor lønnende mål for indsamling af efterretninger og for sabotage, ikke mindst hvis sikkerhedsforanstaltningerne synes at være ineffektive.

SIKKERHEDSFORANSTALTNINGER

6. Hovedformålet med de sikkerhedsforanstaltninger, der er omhandlet i dette afsnit, er at beskytte oplysninger mod uautoriseret indsigt eller ændring og sikre, at de er til rådighed, når de skal anvendes. For at opnå en hensigtsmæssig sikkerhedsbeskyttelse af et SYSTEM, der behandler EU-klassificerede oplysninger, skal de relevante normer for konventionel sikkerhed specificeres tillige med passende specifikke sikkerhedsprocedurer og -teknikker, der er tilpasset det enkelte SYSTEM.

7. Et velovervejet sæt af sikkerhedsforanstaltninger skal fastlægges og gennemføres for at skabe et sikkert miljø for det enkelte SYSTEM. Disse sikkerhedsforanstaltninger skal omfatte fysiske aspekter, personale, ikketekniske foranstaltninger samt procedurer for anvendelse af computer og for kommunikation.

8. Der skal stilles krav om computersikkerhed (sikkerhedsfeatures for både hardware og software) for at sikre overholdelse af princippet om, at kun personer, for hvem indsigt er tjenstlig nødvendig, har adgang til oplysningerne, og for at forebygge eller afsløre uautoriseret offentliggørelse af oplysninger. I hvilket omfang computersikkerhedsforanstaltningerne er tilstrækkelige, skal afgøres under fastsættelsen af sikkerhedskravene. Godkendelsesprocessen skal sikre, at en passende grad af sikkerhed foreligger, så man kan have tillid til computersikkerheden.

SYSTEM-SPECIFIKKE SIKKERHEDSKRAV

9. For alle SYSTEMER, som behandler oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, stilles der en række systemspecifikke sikkerhedskrav, der skal formuleres af de ansvarlige for informationsteknologisystemets drift med indlæsning og nødvendig assistance fra projektpersonalet og INFOSEC-myndigheden som godkendt af godkendel-

▼B

sesmyndigheden. Sådanne systemspecifikke sikkerhedskrav stilles ligeledes, hvis godkendelsesmyndigheden anser uautoriseret indsigt i eller ændring af oplysninger, der er klassificeret RESTREINT UE eller er uklassificerede for at være kritisk.

10. De systemspecifikke sikkerhedskrav udarbejdes på det tidligste stadium af et projekts startfase og udvikles og forstærkes, efterhånden som projektet tager form, så de opfylder forskellige roller på forskellige stadier i projektet og SYSTEMETS livscyklus.

11. De systemspecifikke sikkerhedskrav skal udgøre en bindende aftale mellem informationsteknologisystemets driftsmyndighed og godkendelsesmyndigheden, og SYSTEMET godkendes først, når det opfylder disse krav.

12. De systemspecifikke sikkerhedskrav skal være en fuldstændig og eksplicit fortegnelse over de sikkerhedsprincipper, der skal overholdes, samt over de detaljerede sikkerhedskrav, der skal opfyldes. Grundlaget for disse krav er Rådets sikkerhedspolitik og risikovurdering, medmindre de stilles på grundlag af parametre, der omfatter det operationelle miljø, det laveste sikkerhedsgodkendelsesniveau for personalet, den højeste klassifikationsgrad af de oplysninger, der behandles, sikkerhedsdriftsformen eller brugerkrav. De systemspecifikke sikkerhedskrav er en integrerende del af det dokumentationsprojekt, der skal forelægges for vedkommende myndigheder med henblik på teknisk, budgetmæssig og sikkerhedsmæssig godkendelse. I den endelige form udgør samtlige systemspecifikke sikkerhedskrav en fuldstændig specifikation af SYSTEMETS sikkerhed.

SIKKERHEDSDRIFTSFORMER

13. Alle SYSTEMER, som behandler oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, skal godkendes til at fungere i én, eller hvor det er berettiget, i forskellige tidsperioder, mere end én af følgende sikkerhedsdriftsformer, eller deres tilsvarende nationale sikkerhedsdriftsform:

    a) »dedicated«

    b) »system high«, og

    c) »multilevel«.

Kapitel II

Definitioner

SUPPLERENDE PÅTEGNINGER

14. Supplerende påtegninger som f.eks. CRYPTO eller enhver anden EU-anerkendt særlig behandlingsbetegnelse skal anvendes, hvor der kræves begrænset fordeling og særlig behandling ud over det, der er angivet ved klassifikationsgraden.

15. Ved »DEDICATED«-SIKKERHEDSDRIFTSFORM forstås: en driftsform, hvor ALLE personer med adgang til SYSTEMET er godkendt til den højeste klassifikationsgrad for de oplysninger, der behandles inden for SYSTEMET, og med en generel »need-to-know«-status for SAMTLIGE oplysninger, der behandles inden for SYSTEMET.

    Bemærkninger:

    1) Ved generel »need-to-know«-status forstås, at der ikke er noget obligatorisk krav om computersikkerhedsfeatures, der kan opdele adgangen til oplysningerne inden for SYSTEME.

    2) Andre sikkerhedsfeatures (vedrørende f.eks. fysisk sikring, personale og procedurer) skal være i overensstemmelse med kravene til den højeste klassifikationsgrad og alle kategorier af oplysninger, der behandles inden for SYSTEMET.

16. Ved »SYSTEM HIGH«-SIKKERHEDSDRIFTSFORM forstås: en driftsform, hvor ENHVER, der har adgang til SYSTEMET, er godkendt til den højeste klassifikationsgrad for de oplysninger, der behandles inden for SYSTEMET; ENHVER, der har adgang til SYSTEMET, har dog dermed ikke generel »need-to-know«-status med hensyn til de oplysninger, der behandles inden for SYSTEMET.

    Bemærkninger:

    1) Ved ikke-generel »need-to-know«-status forstås, at det kræves, at de pågældende sikkerhedsfeatures skal give selektiv adgang til eller opdele oplysningerne inden for SYSTEMET.

▼B

2) Andre sikkerhedsfeature (vedrørende f.eks. fysisk sikring, medarbejdere og procedurer) skal være i overensstemmelse med kravene til den højeste klassifikationsgrad og alle kategorier af oplysninger, der behandles inden for SYSTEMET

3) Alle oplysninger, der behandles i eller er tilgængelige for et SYSTEM i henhold til denne driftsform, skal, så længe der ikke er truffet anden afgørelse, sammen med det opnåede resultat beskyttes som værende potentielt af den oplysningskategori og af den højeste klassifikationsgrad, der behandles, medmindre man med rimelighed kan forlade sig på den foreliggende funktionsangivelse.

17. Ved »MULTILEVEL«-SIKKERHEDSDRIFTSFORM forstås: en driftsform, hvor IKKE ALLE personer, der har adgang til SYSTEMET, er godkendt til den højeste klassifikationsgrad for de oplysninger, der behandles inden for SYSTEMET, og hvor ALLE personer, der har adgang til SYSTEMET, ikke generelt har »need-to-know«-status med hensyn til de oplysninger, der behandles inden for SYSTEMET.

Bemærkninger:

1) Denne driftsform gør det for tiden muligt at behandle oplysninger med forskellig klassifikationsgrad og blandede kategorier af oplysninger.

2) Det forhold, at ikke alle er godkendt til de højeste klassifikationsgrader og ikke generelt har »need-to-know«-status, betyder, at der må kræves computersikkerhedsfeatures, der kan give selektiv adgang til og adskillelse af forskellige oplysninger inden for SYSTEMET.

18. Ved INFOSEC forstås: anvendelse af sikkerhedsforanstaltninger, for at oplysninger, der er behandlet, lagret eller videresendt i kommunikations-, informations- og andre elektroniske systemer, kan beskyttes mod uautoriseret indsigt og uautoriseret ændring ved uagtsomhed eller bevidst og sikres, så de er til rådighed, når de skal anvendes, samt for at forebygge uautoriserede ændringer af systemerne og sikre, at de er til rådighed, når de skal anvendes. INFOSEC-foranstaltninger omfatter foranstaltninger med henblik på computer-, transmissions-, emissions- og kryptografisikkerhed samt påvisning, dokumentation og imødegåelse af trusler mod oplysningerne og SYSTEMERNE.

19. Ved COMPUTERSIKKERHED (COMPUSEC) forstås: anvendelse af hardware-, firmware- og softwaresikkerhedsfeatures på et computersystem for at beskytte mod eller forebygge uautoriseret offentliggørelse, manipulering, ændring/sletning af oplysninger, eller at systemet ikke er til rådighed, når det skal anvendes.

20. Ved COMPUTERSIKKERHEDSPRODUKT forstås: et generisk computersikkerhedselement, som inkorporeres i et informationsteknologisystem med henblik på en forstærket eller indbygget sikkerhed for de behandlede oplysninger imod uautoriseret indsigt og uautoriseret ændring samt mod, at systemet ikke er til rådighed, når det skal anvendes.

21. Ved KOMMUNIKATIONSSIKKERHED (COMSEC) forstås: anvendelse af sikkerhedsforanstaltninger på telekommunikation, så uautoriserede personer ikke har adgang til oplysninger af værdi, selv om de måtte besidde eller have undersøgt sådan telekommunikation, eller for at sikre pålideligheden af sådan telekommunikation.

Bemærkning:

Sådanne foranstaltninger omfatter kryptografi-, transmissions- og emissionssikkerhed og omfatter ligeledes procedure-, materiel-, personale-, dokument- og computersikkerhed.

22. Ved EVALUERING forstås: vedkommende myndigheds detaljerede tekniske gennemgang af et SYSTEM eller af et kryptografisk eller et computersikkerhedsprodukts sikkerhedsaspekter.

Bemærkninger:

1) Ved evalueringen undersøges, om den nødvendige sikkerhedsfunktionsdygtighed er til stede, og at der ikke er negative bivirkninger af en sådan funktionsdygtighed, ligesom en sådan funktionsdygtigheds modstandsevne over for indgreb vurderes.

2) Ved evalueringen fastslås det, i hvilket omfang et SYSTEMS sikkerhedskrav eller sikkerhedskravene til et computersikkerhedsprodukt er opfyldt, ligesom sikkerhedsniveauet for SYSTEMET eller det kryptografiske eller computersikkerhedsproduktets pålidelige funktion fastslås.

23. Ved CERTIFICERING forstås: udstedelse af en formel erklæring, der støttes af en uafhængig gennemgang af gennemførelsen og resultaterne af en

▼B

evaluering, om i hvilket omfang et SYSTEM opfylder sikkerhedskravet eller et computersikkerhedsprodukt opfylder forudfastlagte sikkerhedskrav.

24. Ved GODKENDELSE forstås: tilladelse til og godkendelse af et SYSTEM til at behandle EU-klassificerede oplysninger i dets operationelle miljø.

Bemærkning:

En sådan godkendelse foretages, efter at alle relevante sikkerhedsprocedurer er blevet gennemført, og en tilstrækkelig grad af beskyttelse af systemressourcerne er blevet opnået. Godkendelse foretages normalt på grundlag af listen over systemspecifikke sikkerhedskrav, herunder følgende:

a) en erklæring om formålet med godkendelsen af systemet, specielt klassifikationsgraden for de oplysninger, der behandles, og hvilket system eller hvilken operationel netsikkerhed der foreslås

b) fremlæggelse af en risikostyringsundersøgelse til identificering af trusler og sårbarhed og foranstaltninger til at imødegå tvister og sårbarhed

c) sikkerhedsdriftsprocedurer med en detaljeret beskrivelse af de foreslåede operationer (f.eks. måder, tjenester, der skal ydes) og med en beskrivelse af SYSTEMETS sikkerhedsfeatures, som skal udgøre grundlaget for godkendelsen

d) planen for gennemførelse og vedligeholdelse af sikkerhedsfeatures

e) planen for den indledende og efterfølgende systemsikkerheds- og netsikkerhedstest, evaluering og certificering, og

f) eventuelt certificering sammen med andre elementer af godkendelse.

25. Ved INFORMATIONSTEKNOLOGISYSTEM forstås: en samling af udstyr, metoder og procedurer samt eventuelt nødvendigt personale med henblik på at udføre databehandlingsfunktioner.

Bemærkninger:

1) Dette kan betyde en samling af faciliteter, der er opbygget til databehandling inden for systemet.

2) Sådanne systemer kan være til støtte for søgning, styring, kontrol, kommunikation, videnskabelige eller administrative anvendelser, herunder tekstbehandling.

3) Grænserne for et system vil generelt bestemmes som værende de elementer, der kontrolleres af en enkelt informationsteknologisystemdriftsmyndighed.

4) Et informationsteknologisystem kan indeholde undersystemer, hvoraf nogle selv er informationsteknologisystemer.

26. Ved INFORMATIONSTEKNOLOGISYSTEMSIKKERHEDSFEATURES forstås: alle hardware-, firmware- og softwarefunktioner, karakteristika og features; drifts- og ansvarsprocedurer samt adgangskontrol, informationsteknologi-området, området for fjernterminal/arbejdsstation, og styringsbegrænsninger, fysisk struktur og komponenter, medarbejder- og kommunikationskontrol, der er nødvendig for at sikre et acceptabelt beskyttelsesniveau for klassificerede oplysninger, der skal behandles i et informationsteknologisystem.

27. Ved INFORMATIONSTEKNOLOGINET forstås: en geografisk spredt struktur af indbyrdes forbundne informationsteknologisystemer til udveksling af oplysninger, herunder komponenterne i de indbyrdes forbundne informationsteknologisystemer og deres grænseflade med baggrundsdata- og kommunikationsnet.

Bemærkninger:

1) Et informationsteknologinet kan udnytte tjenesterne i et eller flere indbyrdes forbundne kommunikationsnet til udveksling af oplysninger; flere informationsteknologinet kan udnytte tjenesterne i et fælles kommunikationsnet.

2) Et informationsteknologinet kaldes »lokalt«, hvis det forbinder flere computere sammen på samme lokalitet.

28. Ved INFORMATIONSTEKNOLOGINETSIKKERHEDSFEATURES forstås: informationsteknologisystemets sikkerhedsfeatures i de enkelte informationsteknologisystemer, herunder nettet sammen med de yderligere komponenter og features, der er forbundet med nettet som sådan (f.eks. netkommunikation, sikkerhedsidentificering og mærkningsmekanismer samt procedurer, adgangskontrol, programmer og elektronisk identifikation af

▼B

brugerne), og som er nødvendige for at sikre en acceptabel beskyttelsesgrad for klassificerede oplysninger.

29. Ved INFORMATIONSTEKNOLOGIOMRÅDE forstås: et område, som indeholder en eller flere computere, deres lokale ydre enheder og lagringsenheder, kontrolenheder og »dedicated« net og kommunikationsudstyr.

Bemærkning:

Omfatter ikke et særligt område, hvor ydre fjernkomponenter eller terminaler/arbejdsstationer er placeret, uanset om disse komponenter er forbundet til udstyr i informationsteknologi-området.

30. Ved FJERNTERMINAL/ARBEJDSSTATIONSOMRÅDET forstås: et område med computerudstyr, tilhørende lokale ydre komponenter eller terminaler/arbejdsstationer og alt forbundet kommunikationsudstyr, adskilt fra et informationsteknologi-område.

31. Ved TEMPEST-modforanstaltninger forstås: sikkerhedsforanstaltninger, der skal beskytte udstyr og kommunikationsinfrastrukturer mod lækage af klassificerede oplysninger som følge af utilsigtede elektromagnetiske emissioner.

Kapitel III

Sikkerhedsansvar

GENERELT

32. Sikkerhedsudvalgets mandat som defineret i afsnit 1, punkt 4, omfatter bl.a. INFOSEC-spørgsmål. Sikkerhedsudvalget tilrettelægger sine aktiviteter på en sådan måde, at det kan stille ekspertrådgivning til rådighed om ovennævnte spørgsmål.

33. Opstår der problemer vedrørende sikkerhedsbeskyttelsen (uheld, brud på sikkerhedsbestemmelserne, m.v.) skal vedkommende nationale sikkerhedsmyndighed og/eller GSR's Sikkerhedskontor øjeblikkeligt gribe ind. Alle problemer henvises til GSR's Sikkerhedskontor.

34. Generalsekretæren/den højtstående repræsentant eller eventuelt lederen af vedkommende decentrale EU-organ opretter et INFOSEC-kontor, der skal vejlede sikkerhedsmyndigheden om gennemførelsen og kontrollen af særlige sikkerhedsfeatures, der skal være en del af SYSTEMERNE.

SIKKERHEDSGODKENDELSESMYNDIGHED

35. Sikkerhedsgodkendelsesmyndigheden er enten:

— de nationale sikkerhedsmyndigheder

— den myndighed, der er udpeget af generalsekretæren/den højtstående repræsentant

— sikkerhedsmyndigheden i et decentralt EU-organ, eller

— disse myndigheders delegerede/udnævnte repræsentanter, afhængig af hvilket SYSTEM der skal godkendes.

36. Sikkerhedsgodkendelsesmyndigheden er ansvarlig for at sikre SYSTEMERNES overensstemmelse med Rådets sikkerhedspolitik. En af dens opgaver er at godkende SYSTEMER, der skal behandle EU-klassificerede oplysninger med en bestemt klassifikationsgrad i operationelle miljøer. For så vidt angår GSR og eventuelt decentrale EU-organer, er sikkerhedsgodkendelsesmyndigheden ansvarlig for sikkerhed på vegne af generalsekretæren/den højtstående repræsentant eller lederne af vedkommende decentrale organer.

Jurisdiktionen for GSR's sikkerhedsgodkendelsesmyndighed omfatter alle de systemer, der er i drift inden for GSR's bygninger. SYSTEMER og komponenter til SYSTEMER i drift i en medlemsstat forbliver under medlemsstatens egen jurisdiktion. Kommer forskellige komponenter i et SYSTEM ind under både GSR's sikkerhedsgodkendelsesmyndigheds og andre sikkerhedsgodkendelsesmyndigheders jurisdiktion, udpeger parterne en fælles godkendelsesbestyrelse, idet GSR's sikkerhedsgodkendelsesmyndighed står for samordningen.

▼B

INFOSEC-MYNDIGHEDEN

37. INFOSEC-myndigheden er ansvarlig for INFOSEC-kontorets aktiviteter. For så vidt angår GSR og eventuelle decentrale EU-organer, er INFOSEC-myndigheden ansvarlig for:

— at stille teknisk rådgivning og bistand til rådighed for sikkerhedsgodkendelsesmyndigheden

— at medvirke til udviklingen af de systemspecifikke sikkerhedskrav

— at revidere de systemspecifikke sikkerhedskrav, så de er i overensstemmelse med disse sikkerhedsforskrifter og dokumenter om INFOSEC-politikker og -arkitektur

— at deltage i godkendelsespaneler/bestyrelser, hvis det ønskes, og at sørge for INFOSEC-anbefaling om godkendelse til sikkerhedsgodkendelsesmyndigheden

— at sikre støtte til INFOSEC-uddannelsesaktiviteter

— at sikre teknisk rådgivning ved undersøgelsen af uheld, m.v., der vedrører INFOSEC

— at opstille en teknisk politikvejledning for at sikre, at kun godkendt software anvendes.

IT-SYSTEMETS OPERATIVE MYNDIGHED

38. INFOSEC-myndigheden skal tidligst muligt delegere ansvaret for gennemførelsen og driften af kontrol og særlige sikkerhedsfeatures af SYSTEMET til informationsteknologisystemets operative myndighed. Dette ansvar skal i hele SYSTEMETS livscyklus strække sig fra projektudformningsstadiet til det endelige arrangement.

39. Den operative myndighed er ansvarlig for alle de sikkerhedsforanstaltninger, der er bestemt som en del af det generelle SYSTEM. Dette ansvar omfatter forberedelsen af de operative sikkerhedsprocedurer. Myndigheden specificerer sikkerhedsstandarder og sikkerhedspraksis, der skal opfyldes af leverandøren af SYSTEMET.

40. Myndigheden kan eventuelt delegere en del af sit ansvar til f.eks. INFOSEC-sikkerhedsofficeren og INFOSEC-site-sikkerhedsofficeren. De forskellige INFOSEC-funktioner kan udføres af en enkelt person.

BRUGERE

41. Alle brugere er ansvarlige for at sikre, at deres handlinger ikke utilsigtet påvirker sikkerheden af det SYSTEM, de anvender.

INFOSEC-KURSER

42. INFOSEC-kurser skal kunne afholdes på alle niveauer og eventuelt for forskelligt personale inden for GSR, decentrale EU-organer eller medlemsstaternes myndigheder.

Kapitel IV

Ikke-tekniske sikkerhedsforanstaltninger

SIKKERHEDEN OG MEDARBEJDERNE

43. SYSTEMETS brugere skal være sikkerhedsgodkendt og have »need-to-know«-status med hensyn til den klassifikationsgrad og indholdet af de oplysninger, der behandles inden for SYSTEMET. Adgang til visse former for udstyr eller oplysninger, der er specifikke for SYSTEMERNE, kræver særlig godkendelse udstedt i henhold til Rådets procedurer.

44. Sikkerhedsgodkendelsesmyndigheden definerer alle følsomme arbejdsopgaver og specificerer det niveau for godkendelse og kontrol, der kræves foralle medarbejdere, der beskæftiger sig med disse opgaver.

45. SYSTEMERNE specificeres og udformes på en måde, der letter tildelingen af pligter og ansvar tilmedarbejderne, således at en enkelt medarbejder ikke får fuldstændigt kendskab til eller kontrol med sikkerhedssystemets nøglepunkter. Det skal tilstræbes, at en enkelt medarbejder ikke kan foretage ændring eller bevidst nedbrydning af SYSTEMET eller nettet, men at to eller flere medarbejdere er nødt til at samarbejde, hvis et sådant forehavende skal lykkes.

▼B

FYSISK SIKKERHED

46. Informationsteknologi eller områder med fjernterminal/arbejdsstation (som defineret i nr. 29 og 30 ovenfor), hvor oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, behandles af informationsteknologi, eller hvor potentiel adgang til sådanne oplysninger ikke kan udelukkes, skal erklæres EU Klasse I- eller Klasse II-sikkerhedsområder eller eventuelt tilsvarende nationale klasser.

47. Informationsteknologi- eller fjernterminal/arbejdsstationsområder, hvor SYSTEMETS sikkerhed kan ændres, må ikke være bemandet af kun én autoriseret medarbejder.

KONTROL AF ADGANG TIL ET SYSTEM

48. Alle data og alt materiel til adgangskontrol for et SYSTEM skal beskyttes i henhold til ordninger, der svarer til den højeste klassifikationsgrad og kategoribetegnelse for de oplysninger, der åbnes adgang til.

49. Adgangskontroldata og -materiel destrueres som omhandlet i nr. 61-63 i det følgende, hvis sådanne data eller sådant materiel ikke mere anvendes til dette formål.

Kapitel V

Tekniske sikkerhedsforanstaltninger

INFORMATIONSSIKKERHED

50. Det påhviler udstederen af oplysninger at identificere og klassificere alle informationsbærende dokumenter, hvadenten de har form af udskrivning i klarskrift eller databærer. Hver side af klartsprogsudskrivningen forsynes foroven og forneden med angivelse af klassifikationsgrad. Udskrivning, hvadenten den har form af klarskrift eller databærer, skal have samme klassifikationsgrad som den højeste klassifikationsgrad for de oplysninger, der er anvendt til fremstillingen. Den måde, et SYSTEM betjenes på, kan også have indvirkning på klassifikationsgraden for udskrifter fra det.

51. Det påhviler en organisation og de personer, der modtager oplysninger fra den, at overveje problemerne med samling af forskellige dele af oplysninger og de slutninger, man kan nå til ved at sammenholde de forskellige dele, og at afgøre, hvorvidt en højere klassifikationsgrad er relevant for alle oplysningerne.

52. Det forhold, at oplysningerne kan være indeholdt i en signalkode, transmissionskode eller enhver form for binær fremstilling, udgør ikke nogen sikkerhedsbeskyttelse og bør derfor ikke influere på valget af klassifikationsgrad.

53. Hvis oplysninger videregives fra et SYSTEM til et andet, skal de være beskyttet både under videregivelsen og i det modtagende SYSTEM på en måde, der svarer til deres oprindelige klassifikationsgrad og kategori.

54. Alle databærere skal behandles på en måde, der svarer til den højeste klassifikationsgrad for de lagrede oplysninger eller mediemærket og skal hele tiden være beskyttet på passende måde.

55. Genbrugsdatabærere, der anvendes til lagring af EU-klassificerede oplysninger, skal hele tiden have den højeste klassifikationsgrad, de nogensinde er blevet anvendt til, indtil oplysningerne er blevet korrekt nedklassificeret eller afklassificeret og bærerne omklassificeret i overensstemmelse hermed, eller bærerne afklassificeret eller destrueret efter en godkendt GSR-procedure eller national procedure (jf. nr. 61-63 i det følgende).

KONTROL MED OG ANSVAR FOR ADGANG TIL OPLYSNINGER

56. Der foretages automatisk (elektronisk) eller manuel registrering af brugere, der får adgang til oplysninger, som er klassificeret SECRET UE eller højere. Registret opbevares i overensstemmelse med disse sikkerhedsforskrifter.

57. EU-klassificerede udskrivninger, der befinder sig inden for informationsteknologi-området, kan behandles som et klassificeret element og behøver ikke blive registreret, når blot materialet identificeres, forsynes med angivelse af klassifikationsgrad og kontrolleres på en passende måde.

58. Opnås udskrivningerne fra et SYSTEM, der behandler EU-klassificerede oplysninger, og videregiver oplysningerne til et område med fjernterminalarbejdsstation fra et informationsteknologi-område, fastsættes der procedurer, der skal være godkendt af sikkerhedsgodkendelsesmyndigheden, med

▼B

henblik på kontrol af fjernudskrivningen. For klassifikationsgraden SECRET UE eller højere skal sådanne procedurer omfatte specifikke instrukser vedrørende ansvaret for oplysningerne.

BEHANDLING AF OG KONTROL MED TRANSPORTABLE DATABÆRERE

59. Alle transportable databærere, der er klassificeret CONFIDENTIEL UE eller højere, behandles som materiel, for hvilket gælder generelle regler. Det er nødvendigt at tilpasse identifikations- og klassifikationsmærkning til bærernes specifikke fysiske udseende, således at de klart kan genkendes.

60. Brugerne har ansvaret for at sikre, at EU-klassificerede oplysninger kun lagres på bærere med passende klassifikationsmærkning og -beskyttelse. Der fastsættes procedurer til sikring af, at lagring af EU-oplysninger på alle niveauer på sådanne databærere foretages i overensstemmelse med disse sikkerhedsforskrifter.

AFKLASSIFICERING OG DESTRUKTION AF DATABÆRERE

61. Databærere, der anvendes til lagring af EU-klassificerede oplysninger, kan nedklassificeres eller afklassificeres efter godkendte GSR-procedurer eller nationale procedurer.

62. Databærere, hvorpå der har været lagret TRÈS SECRET UE/EU TOP SECRET-oplysninger eller oplysninger af særlig kategori, må ikke afklassificeres eller genanvendes.

63. Hvis databærere ikke må afklassificeres eller genbruges, skal de destrueres efter en godkendt GSR-procedure eller national procedure.

KOMMUNIKATIONSSIKKERHED

64. Hvis EU-klassificerede oplysninger videregives elektromagnetisk, skal der gennemføres særlige foranstaltninger for at beskytte dem imod uautoriseret indsigt og uautoriseret ændring og sikre, at de er til rådighed, når de skal anvendes. Sikkerhedsgodkendelsesmyndigheden fastlægger kravene for beskyttelse mod sporing og aflytning. Oplysninger, der fremsendes i et kommunikationssystem, skal beskyttes på grundlag af kravene om sikring imod uautoriseret indsigt og uautoriseret ændring og sikkerhed for, at de er til rådighed, når de skal anvendes.

65. Kræves der kryptografiske metoder for at opnå beskyttelse imod uautoriseret indsigt og uautoriseret ændring samt sikkerhed for, at oplysningerne er til rådighed, når de skal anvendes, skal sådanne metoder eller produkter i forbindelse hermed godkendes specifikt til formålet af sikkerhedsgodkendelsesmyndigheden.

66. Under videregivelsen skal oplysninger, der er klassificeret SECRET UE eller højere, beskyttes ved hjælp af kryptografiske metoder eller produkter, der er godkendt af Rådet efter anbefaling fra Rådets sikkerhedsudvalg. Under videregivelsen skal oplysninger, der er klassificeret CONFIDENTIEL UE eller RESTREINT UE, beskyttes ved kryptografiske metoder eller produkter, der er godkendt enten af generalsekretæren/den højtstående repræsentant på anbefaling af Rådets sikkerhedsudvalg eller af en medlemsstat.

67. Detaljerede regler for videregivelse af EU-klassificerede oplysninger fastlægges i specifikke sikkerhedsinstruktioner, der godkendes af Rådet på anbefaling af Rådets sikkerhedsudvalg.

68. Under ekstraordinære operative forhold kan oplysninger, der er klassificeret RESTREINT UE, CONFIDENTIEL UE eller SECRET UE, videregives i klart sprog, såfremt der i hvert enkelt tilfælde er givet udtrykkelig bemyndigelse hertil. Sådanne ekstraordinære forhold foreligger:

    a) under forestående eller faktiske krise-, konflikt- eller krigssituationer, og

    b) hvis hurtig levering er af største betydning, og krypteringsmidler ikke er til rådighed, og det skønnes, at de pågældende oplysninger alligevel ikke kan misbruges i tide til at påvirke operationer negativt.

69. Et SYSTEM skal fuldstændig kunne spærre adgang til EU-klassificerede oplysninger på enhver af eller alle sine fjernarbejdsstationer eller -terminaler, hvis det er nødvendigt enten ved fysisk adskillelse eller ved særlige softwarefeatures, der er godkendt af sikkerhedsgodkendelsesmyndigheden.

INSTALLATION OG STRÅLINGSSIKKERHED

70. Den oprindelige installation af SYSTEMER og alle større ændringer i disse specificeres således, at installation udføres af sikkerhedsgodkendte montører under konstant tilsyn af teknisk kvalificerede medarbejdere, som er

▼B

godkendt til at have adgang til EU-klassificerede oplysninger på det niveau, der svarer til den højeste klassifikationsgrad, som SYSTEMET forventes at lagre og behandle.

71. Alt udstyr installeres i overensstemmelse med Rådets gældende sikkerhedspolitik.

72. SYSTEMER, der behandler oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, skal beskyttes på en sådan måde, at deres sikkerhed ikke kan trues af lækage ved udstråling; mht. undersøgelse og kontrol henvises til »TEMPEST«.

73. TEMPEST-modforanstaltninger for installationer i GSR og EU-decentraliserede Organer kontrolleres og godkendes af en TEMPEST-myndighed, der er udpeget af GSR's sikkerhedsmyndighed. For nationale installationer, som behandler EU-klassificerede oplysninger, er den godkendende myndighed den anerkendte nationale TEMPEST-godkendende myndighed.

Kapitel VI

Sikkerhed under behandling

SIKKERHEDSDRIFTSPROCEDURER

74. Sikkerhedsdriftsprocedurerne definerer de principper, der skal følges i sikkerhedsspørgsmål, de driftsprocedurer, der skal følges, samt medarbejderansvar. Sikkerhedsdriftsprocedurerne udarbejdes under ansvar af informationsteknologisystemets driftsmyndighed.

SOFTWAREBESKYTTELSE/KONFIGURATIONSSTYRING

75. Sikkerhedsbeskyttelse af applikationer afgøres på grundlag af en vurdering af sikkerhedsgodkendelsen af applikationen snarere end klassifikationsgraden for de oplysninger, den skal behandle. Softwareudgaver, der er i brug, bør kontrolleres med jævne mellemrum for at sikre, at de fungerer korrekt, og at der ikke er foretaget uautoriserede ændringer.

76. Nye eller ændrede udgaver af software bør ikke anvendes til behandling af EU-klassificerede oplysninger, før de er blevet kontrolleret af informationsteknologisystemets driftsmyndighed.

KONTROL AF, OM DER FINDES SKADELIG SOFTWARE/COMPUTERVIRUS

77. Kontrol af, om der findes skadelig software/computervirus, foretages regelmæssigt i overensstemmelse med sikkerhedsgodkendelsesmyndighedens krav.

78. Alle databærere, der kommer ind i GSR eller decentrale EU-organer eller i medlemsstaterne, skal kontrolleres for, om de indeholder skadelig software eller computervirus, før de indføres i noget SYSTEM.

VEDLIGEHOLDELSE

79. Kontrakter og procedurer for regelmæssig vedligeholdelse og tilkaldevedligeholdelse af SYSTEMER, for hvilke der er udarbejdet systemspecifikke sikkerhedskrav, skal specificere krav og arrangementer for vedligeholdelsespersonale og det anvendte udstyr, der kommer ind på informationsteknologiområdet.

80. Kravene skal klart fremgå af de systemspecifikke sikkerhedskrav, og procedurerne skal klart fremgå af sikkerhedsdriftsprocedurerne. Kontraktvedligeholdelse, der kræver fjerntilslutningsdiagnose, må kun tillades under ekstraordinære omstændigheder under streng kontrol og kun med sikkerhedsgodkendelsesmyndighedens godkendelse.

Kapitel VII

Anskaffelse af materiel

81. Ethvert sikkerhedsprodukt, der skal anvendes sammen med SYSTEMET og som skal anskaffes, bør enten forudgående have været evalueret og certificeret eller bør løbende være under evaluering og certificering af et anerkendt evaluerings- eller certificeringsorgan i henhold til internationale kriterier (som f.eks. de fælles kriterier for sikkerhedsevaluering af informationsteknologi, ref. ISO 15408).

82. Ved beslutningen om, hvorvidt udstyr, specielt databærere, bør leases i stedet for at købes, skal det tages i betragtning dels, at udstyr, der en gang har været anvendt til behandling af EU-klassificerede oplysninger, ikke må

▼B

frigives uden for et passende sikkert miljø uden først at være blevet afklassificeret og godkendt af sikkerhedsgodkendelsesmyndigheden, og dels, at en sådan godkendelse ikke altid er mulig.

GODKENDELSE

83. Alle SYSTEMER, for hvilke der skal opstilles systemspecifikke sikkerhedskrav forud for behandling af EU-klassificerede oplysninger, godkendes af sikkerhedsgodkendelsesmyndigheden på grundlag af de systemspecifikke sikkerhedskrav, sikkerhedsdriftsprocedurer samt enhver anden relevant dokumentation. Undersystemer og fjernterminaler/arbejdsstationer godkendes som en del af alle de SYSTEMER, de er forbundet med. I de tilfælde, hvor et SYSTEM støtter både Rådet og andre organisationer, skal GSR og relevante sikkerhedsmyndigheder gensidigt være enige om godkendelsen.

84. Godkendelsesprocessen kan udføres i overensstemmelse med en godkendelsesstrategi, der er relevant for det specielle SYSTEM, og som er defineret af sikkerhedsgodkendelsesmyndigheden.

EVALUERING OG CERTIFICERING

85. Inden godkendelse skal hardware-, firmware- og softwaresikkerhedsfeatures i et SYSTEM evalueres og certificeres som værende i stand til at beskytte oplysninger af den relevante klassifikationsgrad.

86. Kravene til evaluering og certificering skal indgå i systemplanlægningen og klart fremgå af de systemspecifikke sikkerhedskrav.

87. Evaluerings- og certificeringsprocesserne udføres i overensstemmelse med godkendte retningslinjer og af teknisk kvalificerede og sikkerhedsgodkendte medarbejdere, som handler på vegne af informationsteknologisystemets driftsmyndighed.

88. Holdene kan stilles til rådighed af en udpeget evaluerings- eller certificeringsmyndighed i en medlemsstat eller af dets udpegede repræsentanter, f.eks. en kompetent og sikkerhedsgodkendt leverandør.

89. Graden af de involverede evaluerings- og certificeringsprocesser kan lempes (f.eks. så kun integrationsaspekter involveres), hvis SYSTEMER er baseret på eksisterende nationalt evaluerede og certificerede computersikkerhedsprodukter.

RUTINEKONTROL AF SIKKERHEDSFEATURES MED HENBLIK PÅ FORTSAT GODKENDELSE

90. Informationsteknologisystemets driftsmyndighed kan fastlægge rutinekontrolprocedurer, som skal sikre, at alle sikkerhedsfeatures i SYSTEMET fortsat er gyldige.

91. De typer ændringer, som kræver fornyet godkendelse, eller som kræver forudgående godkendelse af sikkerhedsgodkendelsesmyndigheden, skal klart identificeres i og fremgå af de systemspecifikke sikkerhedskrav. Efter enhver ændring, reparation eller ethvert svigt, som kan have påvirket SYSTEMETS sikkerhedsfeatures, skal informationsteknologisystemets driftsmyndighed sikre, at der foretages kontrol for at sikre, at de pågældende sikkerhedsfeatures virker korrekt. Fortsat godkendelse af SYSTEMET afhænger normalt af, at kontrollen er blevet gennemført med tilfredsstillende resultat.

92. Alle SYSTEMER, hvor der er indført sikkerhedsfeatures, efterses eller undersøges med jævne mellemrum af sikkerhedsgodkendelsesmyndigheden. For så vidt angår SYSTEMER, som behandler TRÈS SECRET UE/EU TOP SECRET-oplysninger eller oplysninger med supplerende angivelser, skal disse eftersyn foretages mindst en gang om året.

Kapitel VIII

Midlertidig eller lejlighedsvis anvendelse

SIKKERHED FOR MIKROCOMPUTERE/PERSONLIGE COMPUTERE

93. Microcomputere/personlige computere (PC'ere) med faste diske (eller andre former for ikke-flygtig hukommelse), der betjenes enten enkeltstående eller i netetablerede konfigurationer og bærbare computeranordninger (f.eks. bærbare PC'ere og elektroniske »notebooks«) med fast harddisk, betragtes som databærere på samme måde som disketter eller andre transportable databærere.

94. Sådant udstyr skal med hensyn til adgang, behandling, lagring og transport have et sikkerhedsbeskyttelsesniveau, der svarer til den højeste klassifikationsgrad for de oplysninger, der nogensinde lagres eller behandles (indtil

▼B

udstyret er blevet nedklassificeret eller afklassificeret i overensstemmelse med godkendte procedurer).

BRUG AF PRIVATEJET INFORMATIONSTEKNOLOGI-UDSTYR TIL OFFICIELT RÅDSARBEJDE

95. Det er forbudt at anvende privatejede transportable databærere, software og informationsteknologihardware (f.eks. PC'ere og bærbare computeranordninger) med lagringskapacitet til behandling af EU-klassificerede oplysninger.

96. Privatejet hardware, software og lagringsenheder må ikke bringes ind på noget Klasse I- eller Klasse II-område, hvor EU-klassificerede oplysninger behandles, uden bemyndigelse fra chefen for GSR's sikkerhedskontor eller en medlemsstats ministerium eller styrelse eller fra det respektive decentrale EU-organ.

ANVENDELSE AF LEVERANDØREJET ELLER NATIONALT LEVERET INFORMATIONSTEKNOLOGI-UDSTYR TIL OFFICIELT RÅDSARBEJDE

97. Anvendelse af leverandørejet informationsteknologi-udstyr og software i organisationer til støtte for officielt rådsarbejde må kun ske efter bemyndigelse fra chefen for GSR's sikkerhedskontor eller en medlemsstats ministerium eller fra det respektive EU-decentrale organ. Det kan ligeledes tillades, at medarbejdere i GSR eller i et decentralt EU-organ anvender nationalt leveret informationsteknologi-udstyr og software; i så fald skal informationsteknologi-udstyret kontrolleres på lige fod med GSR-udstyr. Hvis informationsteknologi-udstyret skal anvendes til behandling af EU-klassificerede oplysninger, skal den relevante sikkerhedsgodkendelsesmyndighed i begge tilfælde høres, således at de elementer af INFOSEC, der gælder for brugen af det pågældende udstyr, tages korrekt i betragtning og gennemføres korrekt.

▼B

AFSNIT XII

VIDEREGIVELSE AF EU-KLASSIFICEREDE OPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

PRINCIPPER FOR VIDEREGIVELSE AF EU-KLASSIFICEREDE OPLYSNINGER

1. Rådet træffer afgørelse om videregivelse af EU-klassificerede oplysninger til tredjelande eller internationale organisationer på grundlag af:

   — arten og indholdet af sådanne oplysninger

   — modtagernes behov for oplysningerne

   — EU's interesse i videregivelsen.

   Udstedermedlemsstaten høres om videregivelsen.

2. Der træffes afgørelse fra sag til sag afhængig af:

   — hvor tæt et samarbejde EU ønsker med de pågældende tredjelande eller internationale organisationer

   — den lid, der kan fæstes til modtagerne, hvilket afhænger af den sikkerhedsbeskyttelse, de pågældende tredjelande eller organisationer vil anvende i forbindelse med de videregivne EU-klassificerede oplysninger samt graden af overensstemmelse mellem modtagernes sikkerhedsregler og de tilsvarende regler i EU; Rådets sikkerhedsudvalg afgiver teknisk udtalelse til Rådet om sådanne spørgsmål.

3. Modtager tredjelande eller internationale organisationer EU-klassificerede oplysninger, skal de samtidig garantere, at oplysningerne ikke vil blive anvendt til andre formål end dem, der ligger til grund for videregivelsen eller udvekslingen af oplysningerne, og at de vil beskytte oplysningerne i overensstemmelse med Rådets anvisninger.

NIVEAUER

4. Træffer Rådet beslutning om, at klassificerede oplysninger kan videregives til eller udveksles med et tredjeland eller en international organisation, afgør det samtidig, hvor tæt et samarbejde, der er muligt. Dette afhænger navnlig af det pågældende tredjelands eller organisationens politik og regler på sikkerhedsområdet.

5. Der opereres med tre samarbejdsniveauer:

   Niveau 1

   Samarbejde med tredjelande eller internationale organisationer, der ligger meget tæt på EU med hensyn til politik og regler på sikkerhedsområdet.

   Niveau 2

   Samarbejde med tredjelande eller internationale organisationer, der afviger markant fra EU med hensyn til politik og regler på sikkerhedsområdet.

   Niveau 3

   Lejlighedsvist samarbejde med tredjelande eller internationale organisationer, hvis politik og regler på sikkerhedsområdet ikke kan vurderes.

6. Det enkelte samarbejdsniveau er bestemmende for, hvilke sikkerhedsregler modtagerne anmodes om at anvende for at beskytte de klassificerede oplysninger, de modtager; i enkelte tilfælde omformuleres reglerne i lyset af den tekniske udtalelse fra Rådets sikkerhedsudvalg. Tillæg 4, 5 og 6 indeholder en detaljeret beskrivelse af disse procedurer og sikkerhedsregler.

AFTALERNE

7. Fastslår Rådet, at der er et permanent eller langsigtet behov for udveksling af klassificerede oplysninger mellem EU og tredjelande eller internationale organisationer, udarbejder det i samarbejde med de pågældende udvekslingspartnere »aftaler om sikkerhedsprocedurer for udveksling af klassificerede oplysninger«, hvori samarbejdets formål og de gensidige regler for beskyttelse af de udvekslede oplysninger fastsættes.

8. I forbindelse med lejlighedsvist niveau 3-samarbejde, som pr. definition er begrænset med hensyn til tid og formål, kan et aftalememorandum med en beskrivelse af arten af de klassificerede oplysninger, der skal udveksles, og de gensidige forpligtelser i forbindelse med oplysningerne, træde i stedet for »aftalen om sikkerhedsprocedurer for udveksling af klassificerede oplysninger«, hvis oplysningerne ikke er klassificeret højere end RESTREINT UE.

▼B

9. Udkast til aftaler om sikkerhedsprocedurer eller aftalememoranda godkendes af Sikkerhedsudvalget, før de forelægges Rådet til afgørelse.

10. De nationale sikkerhedsmyndigheder bistår generalsekretæren/den højtstående repræsentant med at sikre, at de oplysninger, der videregives, anvendes og beskyttes i overensstemmelse med bestemmelserne i aftalerne om sikkerhedsprocedurer eller aftalememorandaene.

▼**M2**

Tillæg 1

Fortegnelse over de nationale sikkerhedsmyndigheder

BELGIEN

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P&S 6
Rue des Petits Carmes 15
B-1000 Bruxelles
Telephone Secretariat: + 32/2/519 05 74
Telephone Presidency: + 32/2/501 82 20
+ 32/2/501 87 10
Fax: + 32/2/519 05 96

DEN TJEKKISKE REPUBLIK

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DANMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telephone: (45) 33 14 88 88
Fax: (45) 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 København Ø
Telephone: (45) 33 32 55 66
Fax: (45) 33 93 13 20

TYSKLAND

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49-1-888 681 15 26
Fax: + 49-1-888 681 558 06

ESTLAND

Eesti Vabariigi Kaitseministeerium
(Ministry of Defence, Republic of Estonia, Department of Security National Security Authority)
Sakala 1
EE-15094 Tallinn
Telephone: + 372/717 00 30
+ 372/717 00 31
+ 372/717 00 77
Fax: + 372/717 00 01

GRÆKENLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
GR-ΣΤΓ 1020 Χολαργός (Αθήνα)
Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)

▼**M2**

Φαξ: (30-210) 642 64 32

(30-210) 652 76 12

[Hellenic National Defence General Staff (HNDGS)]
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Telephone: (30-210) 657 20 09 (office hours)

(30-210) 657 20 10 (office hours)

Fax: (30-210) 642 64 32

(30-210) 652 76 12

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera nacional radial VI, km 8,5
E-28023 Madrid
Telephone: + 34/913 72 57 07

+ 34/913 72 50 27

Fax: + 34/913 72 58 08

FRANKRIG

Secrétariat général de la défense nationale
Service de sécurité de défense (SGDN/SSD)
51, boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telephone: + 33/1/71 75 81 77

Fax: + 33/1/71 75 82 00

IRLAND

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
IRL-Dublin 2
Telephone (353-1) 478 08 22

Fax (353-1) 478 14 84

ITALIEN

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-00187 Roma
Telephone: + 39/06/611 742 66

Fax: + 39/06/488 52 73

CYPERN

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
CY-1432 Λευκωσία
Τηλέφωνα: (357-22) 80 75 69

(357-22) 80 75 19

(357-22) 80 77 64

Φαξ: (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi Street
CY-1432 Nicosia
Telephone: (357-22) 80 75 69

(357-22) 80 75 19

(357-22) 80 77 64

▼M2

Fax: (357-22) 30 23 51

LETLAND

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1013 Riga
Telephone: + 371/702 54 18

Fax: + 371/702 54 54

LITAUEN

Lithuanian National Security Authority
Gedimino ave. 40/1
LT-01110 Vilnius
Telephone: + 370/5/266 32 01

Fax: + 370/5/266 32 00

LUXEMBOURG

Autorité nationale de sécurité
Ministère d'État
Boîte postale 23 79
L-1023 Luxembourg
Telephone: + 352/478 22 10 central

+ 352/478 22 35 direct

Fax: + 352/478 22 43

+ 352/478 22 71

UNGARN

National Security Authority Republic of Hungary
Nemzeti Biztonsági Felügyelet
Pf.: 2
HU-1352 Budapest
Telephone: + 361/346 96 52

Fax: + 361/346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telephone: + 356/21 24 98 44

Fax: + 356/21 23 53 00

NEDERLANDENE

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Nederland
Telephone: (31-70) 320 44 00

Fax: (31-70) 320 07 33

Ministerie van Defensie
Beveiligingsautoriteit (BA)
Postbus 20701
2500 ES DenHaag
Nederland
Telephone: (31-70) 318 70 60

Fax: (31-70) 318 75 22

ØSTRIG

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43-1-531 15 23 96

Fax: + 43-1-531 15 25 08

▼**M2**

POLEN

Wojskowe Służby Informacyjne (Military Information Services
National Security Authority – Military Sphere)
PL-00-909 Warszawa 60
Telephone: + 48/22/684 13 62

Fax: + 48/22/684 10 76

Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency
National Security Authority – Civilian Sphere
Department for the Protection of Classified Information)
ul. Rakowiecka 2A
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60

Fax: + 48/22/585 85 09

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (351) 21 301 17 10

Fax: (351) 21 303 17 11

SLOVENIEN

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information – NSA
Slovenska cesta 5
SI-1000 Ljubljana
Tel.: (386-1) 426 91 20

Faks: (386-1) 426 91 21

SLOVAKIET

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
SK-851 05 Bratislava
Telephone: + 421/2/68 69 23 14

Fax: + 421/2/68 69 17 00

FINLAND

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu 22/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telephone: (358-9) 16 05 53 38

Fax: (358-9) 16 05 53 03

SVERIGE

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telephone: + 46/8/405 54 44

Fax: + 46/8/723 11 76

DET FORENEDE KONGERIGE

UK National Security Authority
PO Box 49359
London, SW1P 1LU
United Kingdom
Telephone (44-207) 930 87 68

Fax (44-207) 821 86 04

▼M2

Tillæg 2

Sammenlignende oversigt over klassifikationsgrader

Klassifikationsgrad i EU og EU's medlemsstater	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Euratom	*Eura — Top Secret*	*Eura — Secret*	*Eura — Confidential*	*Eura — Restricted*
Belgien	Très Secret Zeer geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Den Tjekkiske Republik	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grækenland	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Frankrig	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	nota ([3])
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Cypern	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Letland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M2

Klassifikationsgrad i EU og EU's medlemsstater	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Ungarn	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederlandene	Zeer geheim	Geheim	Confidentieel	Vertrouwelijk
Østrig	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Slovenien	Strogo tajno	Tajno	Zaupno	Interno
Slovakiet	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sverige	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Det Forenede Kongerige	Top Secret	Secret	Confidential	Restricted
Klassifikationsgrad i internationale organisationer	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
WEU	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([1]) Tyskland: VS = Verschlusssache.

([2]) Frankrig: klassifikationsgraden Très secret défense anvendes i forbindelse med statshemmeligheder; ændring kræver bemyndigelse fra premierministeren.

([3]) Frankrig anvender ikke klassifiationsgraden »DIFFUSION RESTREINTE«. Frankrig håndterer og beskytter dokumenter, der bærer mærket »RESTREINT UE« i henhold til gældende nationale love og bestemmelser, som ikke er mindre restriktive end Rådets sikkerhedsforskrifter.

Tillæg 3

Praktisk klassifikationsvejledning

Denne vejledning må ikke opfattes om en ændring af de grundlæggende bestemmelser i afsnit II og III.

Klassifikationsgrad	Hvornår	Hvem	Påskrifter m.v.	Nedklassificering/afklassificering/destruktion	
				hvem	hvornår
TRÈS SECRET UE/EU TOP SECRET Denne klassifikationsgrad anvendes kun til oplysninger og materiale, hvis videregivelse uden bemyndigelse ville kunne forvolde Den Europæiske Unions eller én eller flere medlemsstaters vitale interesser overordentlig alvorlig skade [II, nr. 1].	Ved lækage af oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, er der sandsynlighed for, at: — stabiliteten i EU, i én af medlemsstaterne eller i venligtsindede lande direkte bringes i fare — forbindelserne med venligtsindede regeringer direkte skades i overordentlig alvorlig grad — et stort antal menneskeliv går tabt — medlemsstaternes eller andre bidragyderes operative effektivitet eller overordentlig vigtige sikkerheds- eller efterretningsoperationers fortsatte effektivitet skades i overordentlig alvorlig grad — EU's eller medlemsstaternes økonomi påføres alvorlig langvarig skade.	Medlemsstaterne: personer med særlig bemyndigelse (udstederne) [III, nr. 4]; GSR: personer med særlig bemyndigelse (udstederne) [III, nr. 4], generalsekretæren/den højtstående repræsentant. Udstederen skal angive en dato eller frist, på/inden for hvilken indholdet kan nedklassificeres eller afklassificeres. Hvis der ikke angives en sådan, skal oplysningernes klassifikationsgrad tages op til revision mindst hvert femte år med henblik på at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [III, nr. 10].	Klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET anvendes i forbindelse med dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, og påføres mekanisk eller i hånden, hvor dette er relevant, umiddelbart før forsvarsmærkningen -ESDP [II, nr. 8]. EU-klassifikationsgraden påføres foroven og forneden midt på hver side, og alle sider nummereres. Hvert dokument påføres et referencenummer og en dato; referencenummeret angives på alle sider. Hvis dokumentet skal fordeles i flere eksemplarer, skal hvert eksemplar påføres eksemplarnummer, som anbringespå første side sammen med en angivelse af det samlede sideantal. Evt. bilag angives på første side [VII, nr. 1].	Afklassificering og nedklassificering må kun foretages af udstederen, generalsekretæren/den højtstående repræsentant, som meddeler ændringen til de instanser, som efterfølgende har modtaget originaldokumentet eller et eksemplar heraf [VIII, nr. 9]. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, destrueres af det centrale sekretariat eller et undersekretariat med ansvar herfor. Alle destruerede dokumenter opføres på en destruktionsattest, der undertegnes af den medarbejder, der har til opgave at kontrollere dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET og den medarbejder der overværer destruktionen; sidstnævnte medarbejder skal være sikkerhedsgodkendt på dette niveau. Sådanne destruktioner journaliseres. Sekretariatet opbevarer destruktionsattesterne og fordelingslisten i 10 år [VII, nr. 31].	Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres [VII, nr. 31]. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, herunder alt klassificeret affald, der stammer fra forberedelsen af dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, som f.eks. beskadigede eksemplarer, arbejdstekster, noter og gennemslagspapir destrueres under opsyn af en medarbejder, der er sikkerhedsgodkendt på dette niveau, ved afbrænding, opløsning, makulering eller ved på anden vis, at sikre, at det pågældende materiale reduceres til en uigenkendelig og ikke-restituerbar form [VII, nr. 31, c].

Klassifikationsgrad	Hvornår	Hvem	Påskrifter m.v.	Nedklassificering/afklassificering/destruktion	
				hvem	hvornår
SECRET UE: Denne klassifikationsgrad anvendes kun til oplysninger og materiale, hvis videregivelse uden bemyndigelse ville kunne forvolde Den Europæiske Unions eller én eller flere af dens medlemsstaters vitale interesser alvorlig skade [II, nr. 2].	Ved lækage af oplysninger, der er klassificeret SECRET UE, er der sandsynlighed for: — at der vil opstå internationale spændinger — at forbindelserne med venligtsindede regeringer vil lide alvorlig skade — at det vil true menneskeliv direkte eller i alvorlig grad anfægte den offentlige orden eller den enkeltes sikkerhed eller frihed — at det vil være til alvorlig skade for medlemsstaternes eller andre bidragyderes styrkers operative effektivitet eller sikkerhed eller for meget værdifulde sikkerheds- eller efterretningsoperationers fortsatte effektivitet — at det vil forvolde væsentlig materiel skade for EU's eller en af dets medlemsstaters finansielle, monetære, økonomiske og handelsmæssige interesser.	Medlemsstaterne: autoriserede personer (udstederen) [III, nr. 2]; GSR og EU's decentrale organer: autoriserede personer (udstederen) [III, nr. 2], generaldirektører, generalsekretæren/den højtstående repræsentant. Udstederen skal anføre en dato eller frist, efter hvilken indholdet kan nedklassificeres eller afklassificeres. I modsat fald skal vedkommende tage klassifikationsgraden op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [III, nr. 10].	SECRET UE påføres dokumenter med denne klassifikationsgrad, og, hvor dette er relevant, tilføjes forsvarspåtegningen ESDP mekanisk eller i hånden [II, nr. 8]. EU-klassifikationsgraden anføres midt på hver side foroven og forneden, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato; referencenummeret anføres på hver side. Hvis dokumentet skal fordeles i flere eksemplarer, skal hvert eksemplar have et nummer, som anføres på første side sammen med det samlede sideantal. Evt. bilag anføres på første side [VII, nr. 1].	Afklassificering og nedklassificering må kun foretages af udstederen, generalsekretæren/den højtstående repræsentant, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [III, nr. 9]. Dokumenter, der er klassificeret SECRET UE, destrueres af det sekretariat, der er ansvarligt for disse dokumenter, under tilsyn af en sikkerhedsgodkendt person. Dokumenter, der er klassificeret SECRET UE, og som destrueres, opføres på underskrevne distributionsattester, der opbevares af sekretariatet i mindst tre år tillige med fordelingslisten [VII, nr. 32].	Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres [VII, nr. 31]. Dokumenter, der er klassificeret SECRET UE, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og karbonpapir, destrueres ved afbrænding, opløsning, makulering eller på anden måde reducering til et produkt, der hverken kan genkendes eller rekonstrueres [VII, nr. 31c og 32].

Klassifikationsgrad	Hvornår	Hvem	Påskrifter m.v.	Nedklassificering/afklassificering/destruktion	
				hvem	hvornår
CONFIDENTIEL UE: Denne klassifikationsgrad anvendes til oplysninger og materiale, hvis videregivelse uden bemyndigelse ville kunne forvolde Den Europæiske Unions eller en eller flere af dens medlemsstaters vitale interesser skade [II, nr. 3].	Ved lækage af oplysninger, der er klassificeret CONFIDENTIEL UE, er der sandsynlighed for: — at de diplomatiske forbindelser vil lide materiel skade, dvs. at det vil medføre formelle protester eller andre sanktioner — at det vil anfægte den enkeltes sikkerhed eller frihed — at det vil være til skade for medlemsstaternes eller andre bidragyderes styrkers operative effektivitet eller sikkerhed eller for værdifulde sikkerheds- eller efterretningsoperationers effektivitet — at det vil undergrave større organisationers finansielle levedygtighed i væsentlig grad — at det vil vanskeliggøre efterforskningen af eller gøre det lettere at begå alvorlig kriminalitet — at det i væsentlig grad vil modvirke EU's eller medlemsstaternes finansielle, monetære, økonomiske og handelsmæssige interesser.	Medlemsstaterne: autoriserede personer (udstederen) [III, nr. 2]; GSR og EU's decentrale organer: autoriserede personer (udstederen) [III, nr. 2], generaldirektører, generalsekretæren/den højtstående repræsentant. Udstederen skal anføre en dato eller frist, efter hvilken indholdet kan nedklassificeres eller afklassificeres. I modsat fald skal vedkommende tage klassifikationsgraden op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [III, nr. 10].	CONFIDENTIEL UE påføres dokumenter med denne klassifikationsgrad, og, hvor dette er relevant, tilføjes forsvarspåtegningen ESDP mekanisk eller i hånden eller ved fortryk på registreret papir [II, nr. 8]. EU-klassifikationen anføres midt på hver side foroven og forneden, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato. Evt. bilag anføres på første side [VII, nr. 2].	Afklassificering og nedklassificering må kun foretages af udstederen, generalsekretæren/den højtstående repræsentant, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [III, nr. 9]. Dokumenter, der er klassificeret CONFIDENTIEL UE, destrueres af det sekretariat, der er ansvarligt for disse dokumenter, under tilsyn af en sikkerhedsgodkendt person. Destruktionen registreres efter de nationale bestemmelser og, for så vidt angår GSR eller EU's decentrale organer, efter anvisninger fra generalsekretæren/den højtstående repræsentant [VII, nr. 33].	Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres [VII, nr. 31]. Dokumenter, der er klassificeret CONFIDENTIEL UE, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og karbonpapir, destrueres ved afbrænding, opløsning, makulering eller på anden måde reducering til et produkt, der hverken kan genkendes eller rekonstrueres [VII, nr. 31c og 33].

Klassifikationsgrad	Hvornår	Hvem	Påskrifter m.v.	Nedklassificering/afklassificering/destruktion	
				hvem	hvornår
RESTREINT UE: Denne klassifikationsgrad anvendes til oplysninger og materiale, hvis videregivelse uden bemyndigelse kunne være uheldig for Den Europæiske Unions eller en eller flere af dens medlemsstaters interesser [II, nr. 4].	Ved lækage af oplysninger, der er klassificeret RESTREINT UE, er der sandsynlighed for: — at det vil påvirke de diplomatiske forbindelser negativt — at det vil volde enkeltpersoner alvorlige problemer — at det vil gøre det vanskeligere at opretholde medlemsstaternes eller andre bidragyderes styrkers operative effektivitet eller sikkerhed — at det vil medføre økonomiske tab for enkeltpersoner eller virksomheder eller gøre det lettere for dem at opnå urimelig vinding eller fordel — at det vil være et brud på garanteret tavshedspligt med hensyn til oplysninger fra tredjepart — at det vil være en overtrædelse af lovgivningen om videregivelse af oplysninger — at det vil vanskeliggøre efterforskningen af eller gøre det lettere at begå kriminalitet — at det vil stille EU eller medlemsstaterne ringere i handelsmæssige eller	Medlemsstaterne: autoriserede personer (udstederen) [III, nr. 2]; GSR og EU's decentrale organer: autoriserede personer (udstederen) [III, nr. 2], generaldirektører, generalsekretæren/den højtstående repræsentant. Ophavsmanden skal anføre en dato eller frist, efter hvilken indholdet kan nedklassificeres eller afklassificeres. I modsat fald skal vedkommende tage klassificeringen op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [III, nr. 10].	RESTREINT UE påføres dokumenter med denne klassifikationsgrad, og, hvor det er relevant, indføres forsvarsmærkningen ESDP, der påføres mekanisk eller elektronisk [II, nr. 8]. EU-klassifikationsgraden anføres midt på hver side foroven og forneden, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato [VII, nr. 2].	Afklassificering og nedklassificering må kun foretages af udstederen, generalsekretæren/den højtstående repræsentant, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [III, nr. 9]. Dokumenter, der er klassificeret RESTREINT UE, destrueres af det sekretariat, der er ansvarligt for disse dokumenter, efter de nationale bestemmelser og, for så vidt angår GSR eller EU's decentrale organer, efter anvisninger fra generalsekretæren/den højtstående repræsentant [VII, nr. 34].	Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres [VII, nr. 31].

▼B

Klassifikationsgrad	Hvornår	Hvem	Påskrifter m.v.	Nedklassificering/afklassificering/destruktion	
				hvem	hvornår
	politiske forhandlinger med andre parter — at det vil vanskeliggøre en effektiv udvikling eller gennemførelse af EU-politikker — at det vil undergrave den rette ledelse af EU og dets virksomhed.				

▼B

Tillæg 4

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande eller internationale organisationer

Niveau 1-samarbejde

PROCEDURER

1. Kompetencen til at videregive EU-klassificerede oplysninger til lande, der ikke har undertegnet traktaten om Den Europæiske Union, eller til internationale organisationer, hvis sikkerhedspolitik og -bestemmelser svarer til EU's, tilkommer Rådet.

2. Rådet kan delegere kompetencen til at træffe afgørelse om videregivelse af klassificerede oplysninger. I så fald angives, hvilken type oplysninger der må videregives, og deres klassifikationsgrad, der normalt ikke må være højere end CONFIDENTIEL UE.

3. Medmindre der er indgået en sikkerhedsaftale, fremsættes anmodninger om videregivelse af EU-klassificerede oplysninger til generalsekretæren/den højtstående repræsentant af de pågældende staters eller internationale organisationers sikkerhedsmyndigheder; formålet med videregivelsen skal fremgå af anmodningen tillige med arten af de pågældende oplysninger og deres klassifikationsgrad.

   Anmodning kan ligeledes fremsættes af en medlemsstat eller et af EU's decentrale organer, som måtte ønske EU-klassificerede oplysninger videregivet; formålet med videregivelsen og fordelene herved for EU skal fremgå af anmodningen, med angivelse af arten af de pågældende oplysninger og deres klassifikationsgrad.

4. Anmodningen behandles af GSR, som

   — hører den medlemsstat eller, hvis dette er relevant, det decentrale EU-organ, der er ophavsmand til de oplysninger, der ønskes videregivet

   — tager de nødvendige kontakter til de anmodende staters eller internationale organisationers sikkerhedsmyndigheder for at undersøge, om deres sikkerhedspolitik og -bestemmelser sikrer, at de videregivne klassificerede oplysninger vil blive beskyttet i overensstemmelse med disse sikkerhedsforskrifter

   — indhenter tekniske udtalelser fra medlemsstaternes nationale sikkerhedsmyndigheder om, hvorvidt der kan fæstes lid til de anmodende stater eller internationale organisationer.

5. GSR forelægger anmodningen og Sikkerhedskontorets indstilling for Rådet med henblik på afgørelse.

DE SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

6. Generalsekretæren/den højtstående repræsentant underretter de anmodende stater eller internationale organisationer om, at Rådet har givet bemyndigelse til at videregive EU-klassificerede oplysninger, og fremsender så mange eksemplarer af disse sikkerhedsforskrifter, som det skønnes nødvendigt. Hvis anmodningen er fremsat af en medlemsstat, underretter denne stat modtageren om, at der er givet bemyndigelse til videregivelsen.

   Afgørelsen om videregivelse træder først i kraft, når modtageren skriftligt har erklæret, at vedkommende:

   — ikke vil anvende oplysningerne til andre formål end dem, der er aftalt

   — vil beskytte oplysningerne i overensstemmelse med disse sikkerhedsforskrifter og navnlig nedenstående særlige bestemmelser.

7. *Medarbejdere*

   a) Adgangen til EU-klassificerede oplysninger skal være strengt begrænset til de medarbejdere, for hvem indsigt er tjenstlig nødvendig (»need-to-know«-status).

   b) Alle, der er bemyndiget til at have adgang til oplysninger, der er klassificeret CONFIDENTIEL UE eller højere, skal enten være i besiddelse af en sikkerhedsattest på det relevante niveau eller den tilsvarende sikkerhedsgodkendelse, i begge tilfælde udstedt af deres egen stats myndigheder.

▼B

8. *Fremsendelse af dokumenter*

a) De praktiske procedurer for fremsendelse af dokumenter fastsættes ved aftale på grundlag af bestemmelserne i afsnit VII i disse sikkerhedsforskrifter. De skal navnlig angive, hvilket sekretariat EU-klassificerede oplysninger skal fremsendes til.

b) Hvis de klassificerede oplysninger, som Rådet har givet bemyndigelse til at videregive, omfatter oplysninger, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal den modtagende stat eller internationale organisation oprette et centralt EU-sekretariat og om nødvendigt EU-undersekretariater. Disse sekretariater er underlagt bestemmelserne i afsnit VIII i disse sikkerhedsforskrifter.

9. *Registrering*

Så snart et sekretariat modtager et EU-dokument, der er klassificeret CONFIDENTIEL UE eller højere, skal det opføre dokumentet i et særligt register i organisationen med kolonner for modtagelsesdato, nærmere angivelser om dokumentet (dato, referencenummer og eksemplarnummer), dets klassifikationsgrad, dokumenttitel, modtagerens navn eller stilling, datoen for returnering af modtagelsesbeviset og datoen for dokumentets returnering til EU eller destruktion.

10. *Destruktion*

a) EU-klassificerede dokumenter destrueres efter anvisningerne i afsnit VI. Kopi af destruktionsattesten for dokumenter, der er klassificeret SECRET UE eller TRÈS SECRET UE/EU TOP SECRET, sendes til det EU-sekretariat, der har fremsendt dokumenterne.

b) EU-klassificerede dokumenter skal indgå i den modtagende organisations planer for destruktion af egne klassificerede dokumenter i nød- eller krisesituationer.

11. *Beskyttelse af dokumenter*

Alle forholdsregler skal træffes for at hindre personer uden bemyndigelse i at få adgang til EU-klassificerede oplysninger.

12. *Kopiering, oversættelse og uddrag*

Der må kun tages fotokopier eller udfærdiges oversættelser af dokumenter, der er klassificeret CONFIDENTIEL UE eller SECRET UE efter bemyndigelse fra chefen for vedkommende sikkerhedsorganisation, som skal registrere og kontrollere de pågældende kopier, oversættelser eller uddrag og forsyne dem med de nødvendige påskrifter.

Der må kun gives bemyndigelse til kopiering eller oversættelse af et dokument, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, af den myndighed, der har udstedt dokumentet, og denne skal angive det tilladte antal kopier; hvis det ikke kan fastslås, hvem der er ophavsmand til dokumentet, henvises anmodningen til GSR's Sikkerhedskontor.

13. *Brud på sikkerhedsbestemmelserne*

Hvis der sker brud på sikkerhedsbestemmelserne i forbindelse med et EU-klassificeret dokument, eller der er mistanke om, at der er sket et sådant brud, skal der straks træffes følgende foranstaltninger, medmindre der er indgået en sikkerhedsaftale:

a) der gennemføres en undersøgelse for at fastslå omstændighederne omkring bruddet på sikkerhedsbestemmelserne

b) GSR's Sikkerhedskontor, den nationale sikkerhedsmyndighed og den myndighed, der har udstedt dokumentet, underrettes, eller det angives klart, at sidstnævnte ikke er blevet underrettet, hvis dette ikke er sket

c) der træffes foranstaltning til at begrænse følgerne af bruddet på sikkerhedsbestemmelserne til et minimum

d) der udarbejdes og gennemføres foranstaltninger med henblik på at forebygge gentagelser

e) eventuelle foranstaltninger, der anbefales af GSR's Sikkerhedskontor med henblik på at forebygge gentagelser, gennemføres.

14. *Inspektioner*

GSR's Sikkerhedskontor skal efter aftale med de pågældende stater eller internationale organisationer have tilladelse til at foretage en vurdering af, hvor effektive foranstaltningerne til beskyttelse af videregivne EU-klassificerede oplysninger er.

▼B

15. *Aflæggelse af rapport*

Medmindre der er indgået en sikkerhedsaftale, skal en stat eller international organisation, så længde den er i besiddelse af EU-klassificerede oplysninger, forelægge en årlig rapport på den dato, der blev fastsat, da bemyndigelsen til videregivelse af oplysningerne blev givet, hvori det bekræftes, at disse sikkerhedsforskrifter er blevet overholdt.

▼B

Tillæg 5

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande eller internationale organisationer

Niveau 2-samarbejde

PROCEDURER

1. Kompetencen til at videregive EU-klassificerede oplysninger til tredjelande eller til internationale organisationer, hvis sikkerhedspolitik og -bestemmelser afviger markant fra EU's, tilkommer Rådet. I princippet er den begrænset til oplysninger, der højst er klassificeret SECRET UE eller lavere; den omfatter hverken nationale oplysninger, der er specifikt forbeholdt medlemsstaterne, eller kategorier af EU-klassificerede oplysninger, der er beskyttet med særlig påtegning.

2. Rådet kan delegere kompetencen til at træffe afgørelse om videregivelse af klassificerede oplysninger. I så fald angives, inden for begrænsningerne i punkt 1, hvilken type oplysninger der må videregives, herunder klassifikationsgraden, der normalt ikke må være højere end RESTREINT UE.

3. Medmindre der er indgået en sikkerhedsaftale, fremsættes anmodninger om videregivelse af EU-klassificerede oplysninger til generalsekretæren/den højtstående repræsentant af de pågældende staters eller internationale organisationers sikkerhedsmyndigheder; formålet med videregivelsen skal fremgå af anmodningen tillige med arten af de pågældende oplysninger og deres klassifikationsgrad.

   Anmodning kan ligeledes fremsættes af en medlemsstat eller et af EU's decentrale organer, som måtte ønske EU-klassificerede oplysninger videregivet; formålet med videregivelsen og fordelene herved for EU skal fremgå af anmodningen, med angivelse af arten af de pågældende oplysninger og deres klassifikationsgrad.

4. Anmodningen behandles af GSR, som

   — hører den medlemsstat eller, hvis dette er relevant, det decentrale EU-organ, der er ophavsmand til de oplysninger, der ønskes videregivet

   — tager foreløbig kontakt til de anmodende staters eller internationale organisationers sikkerhedsmyndigheder for at indhente oplysninger om deres sikkerhedspolitik og bestemmelser og navnlig for at udarbejde en sammenlignende oversigt over de klassifikationsgrader, der gælder henholdsvis i EU og i den pågældende stat eller organisation

   — indkalder til møde i Rådets Sikkerhedsudvalg eller, om nødvendigt efter en stiltiende samtykkeprocedure, retter henvendelse til medlemsstaternes nationale sikkerhedsmyndigheder med henblik på at indhente teknisk udtalelse fra Sikkerhedsudvalget.

5. Rådets Sikkerhedsudvalg afgiver teknisk udtalelse om følgende:

   — den lid, der kan fæstes til de anmodende stater eller internationale organisationer med henblik på at vurdere sikkerhedsrisikoen for EU eller dets medlemsstater

   — en vurdering af, om modtageren er i stand til at beskytte klassificerede oplysninger, der videregives af EU

   — forslag til praktiske procedurer for behandling af de EU-klassificerede oplysninger (f.eks. at udarbejde rensede udgaver af en tekst) og dokumenter, der fremsendes (f.eks. at bibeholde eller fjerne EU-klassifikationsangivelsen, en særlig påtegning eller lign.)

   — hvorvidt udstederen bør nedklassificere eller afklassificere oplysningerne, inden de videregives til de pågældende lande eller internationale organisationer ([1]).

6. Generalsekretæren/den højtstående repræsentant forelægger anmodningen for Rådet med henblik på afgørelse tillige med den tekniske udtalelse fra Rådets Sikkerhedsudvalg, som GSR's Sikkerhedskontor har indhentet.

([1]) Dette indebærer, at udstederen anvender proceduren i afsnit III, nr. 9, såfremt samtlige eksemplarer fordeles inden for EU.

▼B

DE SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

7. Generalsekretæren/den højtstående repræsentant underretter de anmodende stater eller internationale organisationer om, at Rådet har givet bemyndigelse til at videregive EU-klassificerede oplysninger, og fremsender en sammenlignende oversigt over de klassifikationsgrader, der gælder henholdsvis i EU og i de pågældende stater eller organisationer. Hvis anmodningen er fremsat af en medlemsstat, underretter denne stat modtageren om, at der er givet bemyndigelse til videregivelsen.

   Afgørelsen om videregivelse træder først i kraft, når modtageren skriftligt har erklæret, at vedkommende:

   — kun vil anvende oplysningerne til de formål, der er aftalt

   — vil beskytte oplysningerne i overensstemmelse med disse sikkerhedsforskrifter.

8. Nedenstående beskyttelsesregler anvendes, medmindre Rådet efter at have indhentet teknisk udtalelse fra Rådets Sikkerhedsudvalg, beslutter at anvende en særlig procedure for behandling af EU-klassificerede dokumenter (fjerne EU-klassifikationsangivelsen, særlig påtegning eller lign.).

   I så fald tilpasses reglerne.

9. *Medarbejdere*

   a) Adgangen til EU-klassificerede oplysninger skal være strengt begrænset til medarbejdere, for hvem indsigt er tjenstlig nødvendig (»need-to-know«-status).

   b) Alle, der er bemyndiget til at have adgang til klassificerede oplysninger, der er videregivet af EU, skal være i besiddelse af en national sikkerhedsgodkendelse eller adgangsbemyndigelse til nationalt klassificerede oplysninger på det relevante niveau svarende til niveauet i EU, jf. den sammenlignende oversigt.

   c) De nationale sikkerhedsgodkendelser eller adgangsbemyndigelser fremsendes, til orientering, til generalsekretæren/den højtstående repræsentant.

10. *Fremsendelse af dokumenter*

   a) De praktiske procedurer for fremsendelse af dokumenter fastsættes ved aftale mellem GSR's Sikkerhedskontor og de modtagende staters eller internationale organisationers sikkerhedsmyndigheder på grundlag af bestemmelserne i afsnit VII i disse sikkerhedsforskrifter. De skal navnlig angive den nøjagtige adresse, som dokumenterne skal fremsendes til, samt de kurer- eller posttjenester, der skal anvendes til fremsendelse af de EU-klassificerede oplysninger.

   b) Dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, skal sendes i dobbelt kuvert. Den inderste kuvert skal mærkes med »EU« og den pågældende klassifikationsgrad. Modtagelsesbevis vedlægges for hvert klassificeret dokument. Modtagelsesbeviset, der ikke i sig selv er klassificeret, må kun indeholde nærmere angivelser om dokumentet (dato, referencenummer og eksemplarnummer) samt sprog, ikke dokumenttitlen.

   c) Den inderste kuvert anbringes derefter i den ydre kuvert, der forsynes med et forsendelsesnummer med henblik på kvittering. Den ydre kuvert må ikke mærkes med klassifikationsgrad.

   d) Et modtagelsesbevis med angivelse af forsendelsesnummeret skal altid gives til kurer- eller posttjenesten.

11. *Registrering ved modtagelse*

   Den modtagende stats nationale sikkerhedsmyndighed eller tilsvarende organ i den stat, der på sine myndigheders vegne modtager de klassificerede oplysninger fra EU, eller den modtagende internationale organisations sikkerhedskontor skal oprette et særligt kontor til registrering af EU-klassificerede oplysninger ved modtagelsen. Registreringen skal omfatte modtagelsesdato, nærmere angivelser om dokumentet (dato, referencenummer og eksemplarnummer), klassifikationsgrad, dokumenttitel, modtagerens navn eller stilling, datoen for returnering af modtagelsesbeviset og datoen for dokumentets returnering til EU eller destruktion.

12. *Returnering af dokumenter*

   Når modtageren returnerer et klassificeret dokument til Rådet eller den medlemsstat, der videregav det, skal vedkommende følge den i nr. 10 ovenfor beskrevne forsendelsesmåde.

▼B

13. *Beskyttelse*

a) Når dokumenterne ikke er i brug, skal de opbevares i penge- eller stålskab m.v., der er godkendt til opbevaring af nationalt klassificeret materiale med samme klassifikationsgrad. Skabet må ikke have nogen ydre angivelse af indholdet, hvortil der kun skal være adgang for personer, der er bemyndiget til at behandle EU-klassificerede oplysninger. Hvis der benyttes kombinationslås, må kombinationen kun kendes af de medarbejdere i den pågældende stat eller organisation, der er bemyndiget til at have adgang til de EU-klassificerede oplysninger, der opbevares i boksen; kombinationen skal ændres hver sjette måned eller hyppigere ved til- eller afgang af medarbejdere, inddragelse af sikkerhedsgodkendelsen for en af de medarbejdere, der kender kombinationen, eller hvis der er risiko for lækage af oplysningerne.

b) EU-klassificerede dokumenter må kun fjernes fra penge- eller stålskabet af de medarbejdere, der er godkendt til at have adgang til de EU-klassificerede dokumenter, og for hvem indsigt er tjenstlig nødvendig (»need-to-know«-status). De er ansvarlige for sikker opbevaring af dokumenterne, så længe de er i deres besiddelse, og navnlig for at sikre, at ingen uden bemyndigelse får adgang til dokumenterne. De skal ligeledes sikre, at dokumenterne opbevares i penge- eller stålskab, når de er færdige med at bruge dem, samt efter arbejdstids ophør.

c) Der må hverken tages fotokopier af et dokument, der er klassificeret som CONFIDENTIEL UE eller højere, eller tages uddrag af det uden bemyndigelse fra GSR's Sikkerhedskontor.

d) Proceduren for hurtig og fuldstændig destruktion af dokumenterne i en nød- eller krisesituation bør fastlægges og bekræftes i samarbejde med GSR's Sikkerhedskontor.

14. *Fysisk sikkerhed*

a) Penge- eller stålskabe m.v. til opbevaring af EU-klassificerede oplysninger skal holdes aflåst, når de ikke er i brug.

b) Når vedligeholdelses- og rengøringspersonale skal have adgang til eller arbejde i et rum, hvor sådanne penge- eller stålskabe befinder sig, skal de hele tiden ledsages af et medlem af den pågældende stats eller organisations sikkerhedsmyndighed eller af den medarbejder, der mere specifikt er ansvarlig for at føre tilsyn med rummets sikkerhed.

c) Uden for normalt arbejdstid (om natten, i weekender og på officielle fridage) skal sikrede bokse, der indeholder EU-klassificerede dokumenter, være beskyttet enten af en vagt eller af et automatisk alarmsystem.

15. *Brud på sikkerhedsbestemmelserne*

Hvis der sker brud på sikkerhedsbestemmelserne i forbindelse med et EU-klassificeret dokument, eller der er mistanke om, at der er sket et sådant brud, skal der straks træffes følgende foranstaltninger:

a) der sendes straks en rapport til GSR's Sikkerhedskontor eller den nationale sikkerhedsmyndighed i den medlemsstat, som har taget initiativ til at fremsende dokumenterne (med kopi til GSR's Sikkerhedskontor),

b) der gennemføres en undersøgelse, hvorefter en fuldstændig rapport sendes til ovennævnte sikkerhedsorgan (jf. litra a)). De fornødne foranstaltninger til afhjælpning af situationen træffes.

16. *Inspektioner*

GSR's Sikkerhedskontor skal efter aftale med de pågældende stater eller internationale organisationer have tilladelse til at foretage en vurdering af, hvor effektive foranstaltningerne til beskyttelse af de videregivne EU-klassificerede oplysninger er.

17. *Aflæggelse af rapport*

Så længe den pågældende stat eller internationale organisation er i besiddelse af EU-klassificerede oplysninger, skal den forelægge en årlig rapport på den dato, der blev fastsat, da bemyndigelsen til videregivelse af oplysningerne blev givet, hvori det bekræftes, at disse sikkerhedsforskrifter er blevet overholdt.

▼B

Tillæg 6

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande eller internationale organisationer

Niveau 3-samarbejde

PROCEDURER

1. Under visse særlige omstændigheder vil Rådet undertiden kunne ønske at samarbejde med stater eller organisationer, der ikke kan frembyde den sikkerhed, der kræves ifølge disse sikkerhedsforskrifter, og som led i dette samarbejde kan det eventuelt være nødvendigt at videregive EU-klassificerede oplysninger. Sådan videregivelse må ikke omfatte nationale oplysninger, der er specifikt forbeholdt medlemsstaterne.

2. Under de omhandlede særlige omstændigheder vil anmodninger om samarbejde med EU, uanset om de fremsættes af tredjelande eller internationale organisationer eller foreslås af medlemsstaterne eller, hvis dette er relevant, EU's decentrale organer, først blive realitetsbehandlet af Rådet, der i det omfang, det er nødvendigt, indhenter udtalelse fra den medlemsstat eller det decentrale organ, der har udstedt oplysningerne. Rådet skal tage stilling til, om det er hensigtsmæssigt at videregive klassificerede oplysninger, vurdere hvorvidt modtageren er tjenstligt berettiget til indsigt (»need-to-know«-status) og afgøre, hvilken type klassificerede oplysninger der må fremsendes.

3. Hvis Rådet tiltræder, at oplysningerne videregives, indkalder generalsekretæren/den højtstående repræsentant til møde i Rådets Sikkerhedsudvalg eller retter om nødvendigt efter en stiltiende samtykkeprocedure henvendelse til medlemsstaternes nationale sikkerhedsmyndigheder med henblik på at indhente teknisk udtalelse fra Sikkerhedsudvalget.

4. Rådets Sikkerhedsudvalg afgiver teknisk udtalelse om følgende:

   a) en vurdering af sikkerhedsrisikoen for EU eller dets medlemsstater

   b) de pågældende oplysningers klassifikationsgrad, på baggrund af deres art

   c) hvorvidt udstederen bør nedklassificere eller afklassificere oplysningerne, inden de videregives til de pågældende lande eller internationale organisationer ([1])

   d) procedurerne for behandling af de pågældende dokumenter (jf. nr. 5 nedenfor)

   e) mulige fremsendelsesmetoder (brug af de offentlige posttjenester, offentlige eller sikrede telekommunikationssystemer, diplomatpost, sikkerhedsgodkendte kurertjenester osv.).

5. De dokumenter, der videregives til de i dette tillæg omhandlede stater eller organisationer, skal i princippet udfærdiges uden henvisning til kilden eller angivelse af EU-klassifikationsgrad. Rådets Sikkerhedsudvalg kan eventuelt anbefale:

   — at der benyttes en særlig påtegning eller kodebetegnelse

   — at der benyttes et særligt klassifikationssystem, der kæder oplysningernes følsomhed sammen med de kontrolforanstaltninger, der kræves af modtageren i forbindelse med fremsendelse af dokumenterne (eksempler i nr. 14).

6. GSR's Sikkerhedskontor forelægger Sikkerhedsudvalgets tekniske udtalelse for Rådet, og i det omfang, det er nødvendigt, vedlægges forslag til den fornødne overdragelse af kompetence med henblik på udførelse af opgaven, navnlig i hastetilfælde.

7. Når Rådet har godkendt videregivelsen af EU-klassificerede oplysninger og de praktiske gennemførelsesprocedurer, tager GSR's Sikkerhedskontor de nødvendige kontakter til den pågældende stats eller organisations sikkerhedsorgan for at lette anvendelsen af de påtænkte sikkerhedsforanstaltninger.

8. GSR's Sikkerhedskontor sender samtlige medlemsstater og, hvis dette er relevant, EU's decentrale organer en oversigt over oplysningernes art og klassifikationsgrad med henblik på sammenligning med angivelse af de

([1]) Dette indebærer, at udstederen anvender proceduren i afsnit III, nr. 9, såfremt samtlige eksemplarer fordeles inden for EU.

▼B

stater og organisationer, som oplysningerne må videregives til i henhold til Rådets afgørelse.

9. Den nationale sikkerhedsmyndighed i den medlemsstat, der videregiver oplysningerne, eller GSR's Sikkerhedskontor træffe alle nødvendige foranstaltninger til at lette en eventuel senere skadesvurdering og gennemgang af procedurerne.

10. Sagen forelægges på ny for Rådet, hvis betingelserne for samarbejdet ændrer sig.

DE SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

11. Generalsekretæren/den højtstående repræsentant underretter de anmodende stater eller internationale organisationer om, at Rådet har givet bemyndigelse til at videregive EU-klassificerede oplysninger, og fremsender de detaljerede sikkerhedsregler, der er foreslået af Rådets Sikkerhedsudvalg og godkendt af Rådet. Hvis anmodningen er fremsat af en medlemsstat, underretter denne stat modtageren om, at der er givet bemyndigelse til videregivelsen.

    Afgørelsen om videregivelse træder først i kraft, når modtageren skriftligt har erklæret, at vedkommende:

    — ikke vil anvende oplysningerne til andre formål end det samarbejde, Rådet har vedtaget

    — vil beskytte oplysningerne i overensstemmelse med de af Rådet stillede krav.

12. *Fremsendelse af dokumenter*

    a) De praktiske procedurer for fremsendelse af dokumenter fastsættes ved aftale mellem GSR's Sikkerhedskontor og de modtagende staters eller internationale organisationers sikkerhedsmyndigheder. De skal navnlig angive den nøjagtige adresse, som dokumenterne skal fremsendes til.

    b) Dokumenter, der er klassificeret CONFIDENTIEL UE eller højere, skal sendes i dobbelt kuvert. Den inderste kuvert skal mærkes med det særlige stempel eller den særlige kodebetegnelse og med den klassifikationsgrad, der er blevet vedtaget for det pågældende dokument. Modtagelsesbevis vedlægges for hvert klassificeret dokument. Modtagelsesbeviset, der ikke i sig selv er klassificeret, må kun indeholde nærmere angivelser om dokumentet (dato, referencenummer og eksemplarnummer) samt sprog, ikke dokumenttitlen.

    c) Den inderste kuvert anbringes derefter i den ydre kuvert, der forsynes med et forsendelsesnummer med henblik på kvittering. Den ydre kuvert må ikke mærkes med klassifikationsgrad.

    d) Et modtagelsesbevis med angivelse af forsendelsesnummeret skal altid gives til kurer- eller posttjenesten.

13. *Registrering ved modtagelse*

    Den modtagende stats nationale sikkerhedsmyndighed eller tilsvarende organ i den stat, der på sine myndigheders vegne modtager de klassificerede oplysninger fra EU, eller den modtagende internationale organisations sikkerhedskontor skal oprette et særligt kontor til registrering af EU-klassificerede oplysninger ved modtagelsen. Registreringen skal omfatte modtagelsesdato, nærmere angivelser om dokumentet (dato, referencenummer og eksemplarnummer), dets klassifikationsgrad, dokumenttitel, modtagerens navn eller stilling, datoen for returnering af modtagelsesbeviset og datoen for dokumentets returnering til EU eller destruktion.

14. *Benyttelse og beskyttelse af de udvekslede klassificerede oplysninger*

    a) Oplysninger, der er klassificeret SECRET UE, skal behandles af særligt udpegede medarbejdere, der er bemyndiget til at få adgang til oplysninger med denne klassifikationsgrad. Oplysningerne skal opbevares i penge- eller stålskabe m.v. af god kvalitet, som kun kan åbnes af de personer, der er bemyndiget til at få adgang til de oplysninger, de indeholder. De områder, hvor sådanne sikrede skabe befinder sig, skal være bevogtet permanent, og der skal indføres et kontrolsystem for at sikre, at kun behørigt bemyndigede personer får adgang til dem. Dokumenter, der er klassificeret SECRET UE, fremsendes med diplomatpost, sikret postforsendelse eller sikrede telekommunikationssystemer. De må kun kopieres med ophavsmandens skriftlige samtykke. Alle eksemplarer skal registreres og overvåges. Der skal udstedes modtagelsesbevis for alle transaktioner i forbindelse med sådanne dokumenter.

▼B

b) Oplysninger, der er klassificeret CONFIDENTIEL UE, skal behandles af særligt udpegede tjenestemænd, der er bemyndiget til at blive informeret om emnet. Dokumenter skal opbevares i aflåste penge- eller stålskabe m. v. i kontrollerede områder.

Oplysninger, der er klassificeret CONFIDENTIEL UE, fremsendes med diplomatpost, militær postforsendelse eller sikrede telekommunikationssystemer. Det modtagende organ må tage kopier, men skal notere antal og distribution i særlige registre.

c) Oplysninger, der er klassificeret som RESTREINT UE, skal behandles i lokaler, hvortil der ikke er adgang for personer uden bemyndigelse, og skal opbevares i aflåste penge- eller stålskabe. Dokumenter kan fremsendes med den offentlige posttjeneste som rekommanderet forsendelse i dobbelt kuvert samt, i nød- eller krisesituationer under igangværende operationer, via de ubeskyttede offentlige telekommunikationssystemer. Modtageren må tage kopier.

d) Oplysninger, der ikke er klassificeret, kræver ingen særlige beskyttelsesforanstaltninger og kan fremsendes med almindelig post og offentlige telekommunikationssystemer. Modtageren må tage kopier.

15. *Destruktion*

Dokumenter, der ikke længere er brug for, destrueres. For så vidt angår dokumenter, der er klassificeret RESTREINT UE eller CONFIDENTIEL UE, skal der gøres notat herom i de særlige registre. For så vidt angår dokumenter, der er klassificeret SECRET UE, skal der udstedes destruktionsattester, som underskrives af to personer, der overværer, at dokumenterne destrueres.

16. *Brud på sikkerhedsbestemmelserne*

Ved lækage af oplysninger, der er klassificeret CONFIDENTIEL UE eller SECRET UE, eller der er mistanke om en sådan lækage, skal den pågældende stats nationale sikkerhedsmyndighed eller den pågældende organisations sikkerhedschef gennemføre en undersøgelse af omstændighederne. Hvis undersøgelsen bekræfter lækagen, skal den myndighed, der er udsteder, underrettes. Der skal træffes de nødvendige foranstaltninger til at afhjælpe mangelfulde procedurer eller opbevaringsmetoder, hvis de er årsagen til lækagen af oplysningerne. Generalsekretæren/den højtstående repræsentant eller den nationale sikkerhedsmyndighed i den medlemsstat, som har videregivet de oplysninger, der er ramt af lækagen, kan anmode modtageren om at redegøre nærmere for undersøgelsen.