De Europæiske Fællesskabers

Tidende

ISSN 0378-6994

L 317

44. årgang

3. december 2001

Dansk udgave

Retsforskrifter

Indhold

DA

De akter, hvis titel er trykt med magre typer, er løbende retsakter inden for landbrugspolitikken og har normalt en begrænset gyldighedsperiode.

Titlen på alle øvrige akter er trykt med fede typer efter en asterisk.

II

(Retsakter hvis offentliggørelse ikke er obligatorisk)

KOMMISSIONEN

KOMMISSIONENS AFGØRELSE
af 29. november 2001
om ændring af dens forretningsorden

(meddelt under nummer K(2001) 3031)

(2001/844/EF, EKSF, Euratom)

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 218, stk. 2,

under henvisning til traktaten om oprettelse af Det Europæiske Kul- og Stålfællesskab, særlig artikel 16,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 131,

under henvisning til traktaten om Den Europæiske Union, særlig artikel 28, stk. 1, og artikel 41, stk. 1 —

TRUFFET FØLGENDE AFGØRELSE:

Artikel 1

Kommissionens sikkerhedsforskrifter, der er knyttet som bilag til denne afgørelse, indsættes herved i Kommissionens forretningsorden som et bilag hertil.

Artikel 2

Denne afgørelse træder i kraft på dagen for offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

Den anvendes fra den 1. december 2001.

Udfærdiget i Bruxelles, den 29. november 2001.

På Kommissionens vegne

Romano PRODI

Formand

BILAG

KOMMISSIONENS FORSKRIFTER OM SIKKERHED

ud fra følgende betragtninger:

(1) For at udbygge Kommissionens virksomhed på områder, som kræver beskyttelse af visse oplysninger, er det hensigtsmæssigt at indføre en overordnet sikkerhedsordning, der omfatter både Kommissionen og de øvrige institutioner, kontorer og agenturer, der er oprettet med hjemmel i EF-traktaten eller traktaten om Den Europæiske Union, samt medlemsstaterne og andre modtagere af oplysninger, der er klassificeret af Den Europæiske Union, i det følgende benævnt »EU-klassificerede oplysninger«.

(2) For at den således fastlagte sikkerhedsordning kan blive effektiv, vil Kommissionen kun videregive EU-klassificerede oplysninger til eksterne organer, der tilsikrer, at de har truffet alle de foranstaltninger, der er nødvendige for at overholde regler, der nøje svarer til disse forskrifter.

(3) Disse forskrifter indskrænker ikke anvendelsen af forordning nr. 3 af 31. juli 1958 om anvendelse af artikel 24 i traktaten om oprettelse af Det Europæiske Atomenergifællesskab [1], Rådets forordning (Euratom, EØF) nr. 1588/90 af 11. juni 1990 om fremsendelse af fortrolige statistiske oplysninger til De Europæiske Fællesskabers Statistiske Kontor [2] eller Kommissionens afgørelse K (95) 1510 endelig udg. af 23. november 1995 om beskyttelse af edb-systemer.

(4) Kommissionens sikkerhedsordning bygger på de principper, der er opstillet i Rådets afgørelse 2001/264/EF af 19. marts 2001 om vedtagelse af Rådets sikkerhedsforskrifter [3], så det sikres, at Unionens beslutningsproces kan fungere tilfredsstillende.

(5) Kommissionen understreger betydningen af, at de øvrige institutioner i relevant omfang følger de forskrifter og standarder for sikkerhedsbeskyttelse, der er nødvendige for at beskytte Unionens og dens medlemsstaters interesser.

(6) Kommissionen erkender behovet for, at den fastlægger sit eget sikkerhedskoncept under hensyntagen til alle sikkerhedsaspekter og til Kommissionens særlige karakter som institution.

(7) Disse forskrifter indskrænker ikke anvendelsen af traktatens artikel 255 eller af Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter [4] —

Artikel 1

Kommissionens sikkerhedsforskrifter er fastsat i bilaget.

Artikel 2

1. Kommissionens medlem med ansvar for sikkerhedsspørgsmål træffer passende foranstaltninger til at sikre, at de i artikel 1 nævnte forskrifter overholdes i Kommissionen, af Kommissionens tjenestemænd og øvrige ansatte, af personale udstationeret ved Kommissionen, samt inden for alle Kommissionens bygninger, herunder dens repræsentationer og kontorer i Unionen og dens delegationer i tredjelande, og af Kommissionens eksterne tjenesteleverandører, i forbindelse med behandling af EU-klassificerede oplysninger.

2. Medlemsstaterne, andre institutioner, organer, kontorer og agenturer, der er oprettet i henhold til eller på grundlag af traktaterne, kan modtage EU-klassificerede oplysninger på betingelse af, at de sikrer, at regler, der nøje svarer til de i artikel 1 nævnte forskrifter, overholdes inden for deres tjenester og deres bygninger i forbindelse med behandling af EU-klassificerede oplysninger, navnlig af følgende personer:

a) medlemmer af medlemsstaternes faste repræsentationer ved EU samt medlemmer af medlemsstaternes delegationer, der deltager i møder i Kommissionen eller dens organer eller i andre kommissionsaktiviteter

b) andre medarbejdere ved medlemsstaternes myndigheder, uanset om de pågældende gør tjeneste på medlemsstaternes område eller i tredjelande, når de behandler EU-klassificerede oplysninger

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

[1] EFT nr. 17/58 af 6.10.1958, s. 406/58.
[2] EFT L 151 af 15.6.1990, s. 1.
[3] EFT L 101 af 11.4.2001, s. 1.
[4] EFT L 145 af 31.5.2001, s. 43.

Artikel 3

Tredjelande, internationale organisationer og andre organer kan modtage EU-klassificerede oplysninger på betingelse af, at de sikrer, at der ved behandlingen af sådanne oplysninger iagttages regler, der nøje svarer til de i artikel 1 nævnte forskrifter.

Artikel 4

I overensstemmelse med de grundlæggende principper og minimumsstandarder for sikkerhed, der er fastsat i bilagets del I, kan Kommissionens medlem med ansvar for sikkerhedsspørgsmål træffe foranstaltninger i henhold til bilagets del II.

Artikel 5

Disse forskrifter træder fra datoen for deres anvendelse i stedet for:

a) Kommissionens afgørelse K (94) 3282 af 30. november 1994 om sikkerhedsforanstaltninger for klassificerede oplysninger, som udarbejdes eller udveksles i forbindelse med Den Europæiske Unions virksomhed

b) Kommissionens afgørelse K (99) 423 af 25. februar 1999 om procedurer, hvorefter tjenestemænd og øvrige ansatte ved Europa-Kommissionen kan sikkerhedsgodkendes med henblik på at få indsigt i klassificerede oplysninger i Kommissionens besiddelse.

Artikel 6

Fra den dato, fra hvilken disse forskrifter anvendes, skal alle klassificerede oplysninger, som Kommissionen indtil da er i besiddelse af, dog med undtagelse af Euratom-klassificerede oplysninger:

a) hvis de er frembragt af Kommissionen, anses for at være omklassificeret til »EU-RESTRICTED«, medmindre forfatteren beslutter at give dem en anden klassifikationsgrad inden den 31. januar 2002; i så fald skal forfatteren give underretning herom til alle dokumentets adressater

b) hvis de er frembragt af personer uden for Kommissionen, beholde deres oprindelige klassifikationsgrad og således behandles som EU-klassificerede oplysninger af tilsvarende klassifikationsgrad, medmindre forfatteren giver samtykke til afklassificering eller nedklassificering af oplysningerne.

BILAG

SIKKERHEDSFORSKRIFTER

Indholdsfortegnelse

-

DEL I: GRUNDLÆGGENDE PRINCIPPER OG MINIMUMSSTANDARDER FOR SIKKERHED

1. INDLEDNING

I disse forskrifter fastlægges de grundlæggende principper og minimumsstandarder for sikkerhedsbeskyttelse og den måde, hvorpå disse skal overholdes ikke blot af Kommissionen på alle dens tjenestesteder, men også af alle modtagere af EU-klassificerede oplysninger, for at værne om sikkerheden og for at sikre, at der gælder en fælles standard for sikkerhedsbeskyttelse.

2. GENERELLE PRINCIPPER

Kommissionens sikkerhedspolitik indgår som en integrerende del af dens almindelige interne forvaltningspolitik og er dermed baseret på de principper, der gælder for dens almindelige politik:

Disse principper omfatter bl.a. legalitet, åbenhed, ansvarlighed og subsidiaritet (forholdsmæssighed).

Legalitet betyder, at de gældende rammebestemmelser nøje skal iagttages ved udøvelsen af sikkerhedsfunktionerne, og at alle de i bestemmelserne fastsatte krav skal opfyldes. Det betyder også, at ansvarsområderne vedrørende sikkerhed skal have hjemmel i gældende bestemmelser. Personalevedtægtens bestemmelser finder fuld anvendelse, navnlig artikel 17 om personalets forpligtelse til ikke at videregive oplysninger fra Kommissionen og afsnit VI om disciplinærordningen. Endelig betyder det, at brud på sikkerhedsbestemmelserne inden for Kommissionens ansvarsområde skal behandles i overensstemmelse med Kommissionens politik vedrørende disciplinarforanstaltninger og dens politik for samarbejde med medlemsstaterne med hensyn til strafferetlig forfølgning.

Åbenhed betyder, at der skal herske klarhed med hensyn til alle sikkerhedsregler og -forskrifter, så der opnås en ensartet anvendelse heraf i de forskellige tjenestegrene og på de forskellige områder (fysisk sikkerhed sammenholdt med beskyttelse af oplysninger osv.), og at der skal føres en sammenhængende og veltilrettelagt bevidstgørelsespolitik med hensyn til sikkerheden. Det indebærer også, at der er behov for klare skriftlige retningslinjer for gennemførelsen af sikkerhedsforanstaltninger.

Ansvarlighed betyder, at opgaverne på sikkerhedsområdet skal defineres klart. Desuden betyder det, at det regelmæssigt skal kontrolleres, om disse opgaver er blevet udført korrekt.

Subsidiaritet eller forholdsmæssighed betyder, at sikkerheden skal tilrettelægges på det lavest mulige niveau og så nært som muligt på Kommissionens generaldirektorater og tjenester. Det betyder også, at sikkerhedsaktiviteterne skal begrænses til de elementer, hvor der virkeligt er et behov. Og endelig betyder det, at sikkerhedsforanstaltningerne skal stå i forhold til de interesser, der skal beskyttes, og til den faktiske eller potentielle trussel mod disse interesser, så der gives mulighed for at træffe de forholdsregler, der medfører de mindst mulige forstyrrelser.

3. GRUNDLAGET FOR SIKKERHEDSBESKYTTELSE

Grundlaget for en effektiv sikkerhedsbeskyttelse er:

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

   1) at indsamle og registrere efterretninger om spionage, sabotage, terrorisme og anden undergravende virksomhed, og

   2) at underrette og rådgive regeringerne og derigennem Kommissionen om karakteren af de bestående sikkerhedsrisici og om modforholdsregler

b) at der både i hver medlemsstat og i Kommissionen 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 og de relevante tjenestegrene i EU-institutionerne med henblik på alt efter omstændighederne at fastslå eller anbefale:

   1) hvilke personer, oplysninger og ressourcer det er nødvendigt at beskytte, og

   2) fælles standarder for sikkerhedsbeskyttelse

d) at der er et nært samarbejde mellem Kommissionens Sikkerhedskontor og sikkerhedsorganerne ved de øvrige EU-institutioner samt med NATO's Office of Security (NOS).

4. PRINCIPPERNE FOR INFORMATIONSSIKKERHED

4.1. **Formål**

Informationssikkerhedens 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 adgang og ændring og for, at de ikke er til rådighed, når de skal anvendes

c) at beskytte Kommissionens bygninger, 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.

4.2. **Definitioner**

I disse forskrifter forstås ved:

a) »EU-klassificerede oplysninger«: alle oplysninger og ethvert materiale, der i tilfælde af videregivelse uden dertil indhentet bemyndigelse i forskellig grad ville kunne skade EU's interesser eller en eller flere af EU's medlemsstater, uanset om sådanne oplysninger eller sådant materiale er udarbejdet af EU eller modtaget fra medlemsstater, tredjelande eller internationale organisationer

b) »dokument«: enhver form for skrivelse, note, referat, rapport, memorandum, signal/meddelelse, skitse, fotografi, 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

c) »materiale«: et dokument som defineret i litra b) samt alle former for udstyr, både færdigfremstillet og under fremstilling

d) »need to know«: en bestemt medarbejders behov for at få adgang til EU-klassificerede oplysninger for at kunne varetage sin funktion eller udføre sin opgave

e) »godkendelse«: en beslutning truffet af Kommissionens formand om at give en enkeltperson adgang til EU-klassificerede oplysninger op til et bestemt niveau, efter at en sikkerhedsundersøgelse foretaget af en national sikkerhedsmyndighed i henhold til den nationale lovgivning har givet et positivt resultat

f) »klassificering«: fastsættelse af det relevante sikkerhedsniveau for oplysninger, hvis videregivelse uden dertil indhentet bemyndigelse kan være til en vis skade for Kommissionens eller medlemsstaternes interesser

g) »nedklassificering«: fastsættelse af en lavere klassifikationsgrad end den hidtil gældende

h) »afklassificering«: ophævelse af enhver form for klassificering

i) »udsteder«: den behørigt bemyndigede forfatter af et klassificeret dokument; i Kommissionen kan afdelingscheferne give deres personale godkendelse til at udstede EU-klassificerede oplysninger

j) »Kommissionens afdelinger«: Kommissionens afdelinger og tjenestegrene, herunder kabinetterne, på alle arbejdssteder, herunder Det Fælles Forskningscenter, repræsentationer og kontorer i Unionen og delegationer i tredjelande.

4.3. **Klassificering**

a) 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 eller for lav klassifikationsgrad.

b) Klassificeringsordningen er det instrument, hvormed disse principper skal gennemføres; der anvendes en tilsvarende klassificeringsordning ved 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.

c) Ansvaret for klassificering af oplysninger påhviler alene udstederen af de pågældende oplysninger.

d) Klassifikationsgraden baseres alene på indholdet af de pågældende oplysninger.

e) Hvis flere dokumenter med oplysninger grupperes, skal klassifikationsgraden for det samlede materiale mindst være lige så høj som den højeste af de enkelte klassifikationsgrader. En samling af oplysninger kan dog gives en højere klassifikationsgrad end de enkelte dele.

f) Oplysninger klassificeres kun i det omfang og kun så længe, det er nødvendigt.

4.4. **Sikkerhedsforanstaltningernes formål**

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 kan udgøre en sikkerhedsmæssig risiko for klassificerede oplysninger og vigtige anlæg, der rummer klassificerede oplysninger, og enten forhindre, at de får adgang hertil, eller sørge for, at de flyttes fra det pågældende sted

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

d) sikre, at klassificerede oplysninger kun videregives til personer på grundlag af »need-to-know«-princippet, som er af grundlæggende betydning for alle sikkerhedsaspekter

e) sikre alle oplysningers integritet (dvs. hindre forvanskning eller uautoriseret ændring eller slettelse) 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.

5. TILRETTELÆGGELSE AF SIKKERHEDSBESKYTTELSEN

5.1. **Fælles minimumsstandarder**

Kommissionen sikrer, at alle modtagere af EU-klassificerede oplysninger, det være sig i institutionen eller under dens kompetenceområde, herunder alle afdelinger og tjenesteleverandører, overholder fælles minimumsstandarder for sikkerhed, så EU-klassificerede oplysninger kan videregives i tillid til, at de vil blive sikret på passende vis. Disse minimumsstandarder skal omfatte kriterier for sikkerhedsgodkendelse af personale samt procedurer for beskyttelse af EU-klassificerede oplysninger.

Kommissionen giver kun eksterne organer adgang til EU-klassificerede oplysninger på betingelse af, at de sikrer, at der ved behandlingen af EU-klassificerede oplysninger iagttages bestemmelser, der i det mindste nøje svarer til disse minimumsstandarder.

5.2. **Tilrettelæggelse**

Inden for Kommissionen tilrettelægges sikkerhedsbeskyttelsen på to niveauer:

a) På Kommissionens overordnede niveau er det Kommissionens Sikkerhedskontor med en sikkerhedsgodkendelsesmyndighed, der også fungerer som krypteringsmyndighed og som TEMPEST-myndighed, og med en INFOSEC-myndighed og et eller flere centrale sekretariater for EU-klassificerede oplysninger, hvert med en eller flere sekretariatsledere.

b) I Kommissionens enkelte afdelinger henhører ansvaret for sikkerheden under en eller flere lokale sikkerhedsansvarlige, en eller flere centrale edb-sikkerhedsansvarlige, lokale edb-sikkerhedsansvarlige og lokale sekretariater for EU-klassificerede oplysninger med en eller flere sekretariatsledere.

c) De centrale sikkerhedsorganer giver vejledning til de lokale sikkerhedsorganer.

6. MEDARBEJDERNE OG SIKKERHEDSBESKYTTELSEN

6.1. **Sikkerhedsgodkendelse af medarbejdere**

Alle medarbejdere, som skal have indsigt i oplysninger, der er klassificeret EU CONFIDENTIAL 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 er modtagelige for pres fra udenlandsk eller anden side.

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

d) skal have adgang til oplysninger, der er klassificeret EU TOP SECRET

e) beklæder stillinger, som indebærer, at de regelmæssigt skal have adgang til betydelige mængder af oplysninger, der er klassificeret EU SECRET

f) har særlig tjenstlig adgang til sikre kommunikations- og informationssystemer og dermed vil have mulighed for at skaffe sig uautoriseret adgang til store mængder EU-klassificerede oplysninger eller for at forvolde betydelig skade gennem tekniske sabotagehandlinger.

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

Når personer (f.eks. kontorbude, sikkerhedsvagter, vedligeholdelses- og rengøringspersonale), der ikke har »need to know«-status, er nødt til at arbejde under forhold, hvor de kan få adgang til EU-klassificerede oplysninger, skal de forinden være sikkerhedsgodkendt til den relevante klassifikationsgrad.

6.2. **Liste over sikkerhedsgodkendte personer**

Alle Kommissionens afdelinger, der behandler EU-klassificerede oplysninger eller rummer kommunikations- og informationssystemer, 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. Den lokale sikkerhedsansvarlige i den pågældende afdeling ved Kommissionen skal have en liste over de sikkerhedsgodkendte medarbejdere inden for vedkommendes område.

6.3. **Sikkerhedsinstruks til medarbejderne**

Alle medarbejdere, der varetager opgaver, hvor de kan få adgang til klassificerede oplysninger, skal, inden de påbegynder arbejdet og derefter regelmæssigt, modtage en indgående instruks om nødvendigheden af sikkerhedsbeskyttelsen og procedurerne for gennemførelsen heraf. Sådanne medarbejdere skal skriftligt attestere, at de har læst og fuldt ud forstået nærværende sikkerhedsbestemmelser.

6.4. **Ledelsens ansvar**

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

6.5. **Medarbejdernes sikkerhedsstatus**

Der indføres procedurer for at sikre, at der, hvis der fremkommer negative oplysninger om en medarbejder, bliver taget stilling til, om den pågældende behandler klassificerede oplysninger eller har adgang til sikre kommunikations- og informationssystemer, og at Kommissionens Sikkerhedskontor underrettes. Hvis det bekræftes, at medarbejderen udgør en sikkerhedsrisiko, skal den pågældende udelukkes fra eller fratages arbejdsopgaver, hvor vedkommende kan være til fare for sikkerheden.

7. FYSISK SIKKERHED

7.1. **Behovet for sikkerhedsbeskyttelse**

Graden af de fysiske foranstaltninger, der skal bringes i anvendelse for at sikre beskyttelsen af EU-klassificerede oplysninger, skal stå i forhold til klassifikationsgraden og til omfanget af og truslen mod de oplysninger og det materiale, det drejer sig om. 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.

7.2. **Kontrol**

Medarbejdere, der fører opsigt med områder med EU-klassificerede oplysninger, og som forlader disse, skal sikre sig, at oplysningerne opbevares forsvarligt, og at alle sikkerhedsanordninger er aktiveret (låse, alarmsystemer osv.). Herudover foretages der efter arbejdstids ophør kontrol af, om disse krav er opfyldt.

7.3. **Sikkerhedsbeskyttelse af bygninger**

Bygninger, der rummer EU-klassificerede oplysninger eller sikre kommunikations- og informationssystemer, skal beskyttes mod uautoriseret adgang. Hvordan EU-klassificerede oplysninger skal beskyttes, det være sig med gitre for vinduer, låse på døre, vagtposter 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 sikre skabe eller bokse, hvor oplysningerne eller materialet opbevares, og

c) bygningens fysiske beskaffenhed og beliggenhed.

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

7.4. **Beredskabsplaner**

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

8. INFORMATIONSSIKKERHED

Informationssikkerheden (INFOSEC) omfatter fastlæggelse og iværksættelse af sikkerhedsforanstaltninger, der kan sikre, at EU-klassificerede oplysninger, der behandles, lagres eller videregives via kommunikations- eller informationssystemer eller via andre elektroniske systemer, ikke hverken uagtsomt eller forsætligt kommer ikke-bemyndigede i hænde eller ændres eller bliver utilgængelige. Der skal træffes fyldestgørende modforanstaltninger for at forhindre, at uautoriserede brugere får adgang til EU-klassificerede oplysninger, eller at autoriserede brugere nægtes adgang til EU-klassificerede oplysninger, samt for at forebygge, at EU-klassificerede oplysninger forvanskes, eller at de ændres eller slettes uden bemyndigelse.

9. FOREBYGGELSE AF SABOTAGE OG ANDRE FORMER FOR FORSÆTLIG SKADE

Fysiske forholdsregler til beskyttelse af vigtige anlæg med klassificerede oplysninger er de bedst egnede sikkerhedsforanstaltninger, der kan træffes mod sabotage og anden forsætlig skade, og sikkerhedsgodkendelse af personalet er ikke i sig selv nok. Det relevante nationale sikkerhedsorgan skal anmodes om at give oplysninger om spionage, sabotage, terrorisme og anden undergravende virksomhed.

10. VIDEREGIVELSE AF KLASSIFICEREDE OPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

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

Modtager Kommissionen klassificerede oplysninger fra tredjelande, internationale organisationer eller anden tredjepart, skal de pågældende oplysninger beskyttes i overensstemmelse med deres klassifikationsgrad og de standarder, der ifølge nærværende forskrifter gælder for EU-klassificerede oplysninger, eller eventuelt højere standarder, som den tredjepart, der meddeler oplysningerne, måtte stille krav om. Der kan åbnes mulighed for gensidig kontrol.

Ovennævnte principper gennemføres i overensstemmelse med de nærmere bestemmelser i del II, afsnit 26, og tillæg 3, 4 og 5.

DEL II: TILRETTELÆGGELSEN AF SIKKERHEDSBESKYTTELSEN I KOMMISSIONEN

11. KOMMISSIONENS MEDLEM MED ANSVAR FOR SIKKERHEDSSPØRGSMÅL

Det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, skal:

a) gennemføre Kommissionens sikkerhedspolitik

b) tage stilling til sikkerhedsproblemer, der forelægges ham af Kommissionen eller dens kompetente organer

c) behandle spørgsmål, der indebærer ændringer i Kommissionens sikkerhedspolitik, i nær kontakt med medlemsstaternes nationale sikkerhedsmyndigheder (eller andre relevante myndigheder).

Det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, er navnlig ansvarlig for:

a) at samordne alle sikkerhedsspørgsmål, der vedrører Kommissionens virksomhed

b) at anmode de af medlemsstaterne udpegede myndigheder om, at de nationale sikkerhedsmyndigheder foretager sikkerhedsgodkendelse af personale, der arbejder i Kommissionen, jf. afsnit 20

c) 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 Kommissionen

d) at anmode de relevante sikkerhedsmyndigheder om at iværksætte efterforskning, hvis uautoriseret videregivelse af EU-klassificerede oplysninger forekommer at være sket uden for Kommissionen, og at samordne efterforskningen, hvis mere end én sikkerhedsmyndighed er involveret

e) at der regelmæssigt foretages en gennemgang af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger

f) at holde løbende kontakt med alle relevante sikkerhedsmyndigheder med henblik på at opnå en overordnet samordning af sikkerhedsbeskyttelsen

g) løbende at tage Kommissionens sikkerhedspolitik og -procedurer op til nyvurdering og i givet fald at udarbejde relevante henstillinger. Kommissionens medlem med ansvar for sikkerhedsspørgsmål forelægger i den forbindelse Kommissionen den årlige inspektionsplan, der udarbejdes af Kommissionens Sikkerhedskontor.

12. KOMMISSIONENS RÅDGIVENDE GRUPPE FOR SIKKERHEDSPOLITIK

Der oprettes ved Kommissionen en rådgivende gruppe for sikkerhedspolitik. Den omfatter det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, eller vedkommendes stedfortræder, som varetager formandsposten, og repræsentanter for de enkelte medlemsstaters nationale sikkerhedsmyndigheder. Repræsentanter for de øvrige EU-institutioner kan også indbydes til at deltage. Repræsentanter for de relevante decentrale EF- og EU-organer kan også indbydes til at deltage, når der drøftes spørgsmål, som berører disse.

Kommissionens Rådgivende Gruppe for Sikkerhedspolitik mødes på formandens initiativ eller efter anmodning fra et af gruppens medlemmer. Gruppen har til opgave at gennemgå og vurdere alle relevante sikkerhedsspørgsmål og i givet fald at forelægge Kommissionen henstillinger.

13. KOMMISSIONENS SIKKERHEDSRÅD

Der oprettes ved Kommissionen et sikkerhedsråd. Det omfatter generalsekretæren, som varetager formandsposten, og generaldirektørerne for Den Juridiske Tjeneste, Personale og Administration, Eksterne Forbindelser, Retlige og Indre Anliggender og Det Fælles Forskningscenter og cheferne for Den Interne Revisionstjeneste og Kommissionens Sikkerhedskontor. Andre tjenestemænd i Kommissionen kan indbydes til at deltage. Dets opgave er at vurdere sikkerhedsforanstaltningerne inden for Kommissionen og at fremsætte henstillinger på dette område til Kommissionens medlem med ansvar for sikkerhedsspørgsmål.

14. KOMMISSIONENS SIKKERHEDSKONTOR

Med henblik på udførelsen af de opgaver, der er nævnt i afsnit 11, kan Kommissionens medlem med ansvar for sikkerhedsspørgsmål pålægge Kommissionens Sikkerhedskontor at samordne, føre tilsyn med og gennemføre sikkerhedsforanstaltninger.

Chefen for Kommissionens Sikkerhedskontor er den ledende konsulent i sikkerhedsspørgsmål for det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, og fungerer som sekretær for Den Rådgivende Gruppe for Sikkerhedspolitik. I den forbindelse forestår vedkommende ajourføringen af sikkerhedsforskrifterne og samordner sikkerhedsforanstaltningerne med medlemsstaternes myndigheder samt i relevant omfang med internationale organisationer, der har sikkerhedsaftaler med Kommissionen. Med henblik herpå fungerer vedkommende som kontaktperson.

Chefen for Kommissionens Sikkerhedskontor er ansvarlig for godkendelsen af IT-systemer og -netværk i Kommissionen. Chefen for Kommissionens Sikkerhedskontor træffer efter aftale med de relevante nationale sikkerhedsmyndigheder beslutning om godkendelsen af IT-systemer og -netværk, der omfatter både Kommissionen og andre modtagere af EU-klassificerede oplysninger.

15. SIKKERHEDSINSPEKTIONER

Kommissionens Sikkerhedskontor gennemfører regelmæssige inspektioner af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger.

Kommissionens Sikkerhedskontor kan i den forbindelse bistås af sikkerhedstjenesterne i andre EU-institutioner, der ligger inde med EU-klassificerede oplysninger, og af medlemsstaternes nationale sikkerhedsmyndigheder [1].

På anmodning af en medlemsstat kan dens nationale sikkerhedsmyndighed sammen med Kommissionens Sikkerhedskontor efter aftale foretage inspektion af EU-klassificerede oplysninger i Kommissionen.

[1] Med forbehold for Wiener-konventionen af 1961 om diplomatiske forbindelser og protokollen af 8. april 1965 vedrørende De Europæiske Fællesskabers privilegier og immuniteter.

16. KLASSIFIKATIONSGRADER, SIKKERHEDSANGIVELSER OG PÅTEGNINGER

16.1. **Klassifikationsgrader** [1]

Oplysninger klassificeres således (se også tillæg 2):

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.

EU 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 alvorlig skade.

EU CONFIDENTIAL: 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.

EU RESTRICTED: 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.

Der må ikke anvendes andre klassifikationsgrader.

16.2. **Sikkerhedsangivelser**

Til begrænsning af gyldighedsperioden for en klassifikationsgrad (angivelse af automatisk nedklassificering eller afklassificering af klassificerede oplysninger) kan der benyttes en godkendt sikkerhedsangivelse. Angivelsen skal være enten »UNTIL …..(tid/dato)« eller »UNTIL ….(begivenhed)«.

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

Sikkerhedsangivelser må kun benyttes i forbindelse med en klassifikationsgrad.

16.3. **Påtegninger**

Det kan med en særlig påtegning angives, hvilket område dokumentet omhandler, hvordan det skal fordeles efter »need-to-know«-princippet, eller hvornår en embargo ophører (for ikke-klassificerede oplysninger).

En påtegning er ikke en klassifikationsgrad og må ikke anvendes i stedet for en sådan.

Betegnelsen ESDP 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.

16.4. **Anførelse af klassifikationsgrad**

Klassifikationsgraden anføres således:

a) på dokumenter, der er klassificeret EU RESTRICTED: mekanisk eller elektronisk

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

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

16.5. **Anførelse af sikkerhedspåtegninger**

Sikkerhedspåtegninger anføres direkte under klassifikationsgraden på samme måde som ved anførelse af klassifikationsgrad.

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

17. KLASSIFIKATIONSSTYRING

17.1. **Generelt**

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

Ansvaret for klassificering af oplysninger og for eventuel senere nedklassificering eller afklassificering påhviler alene udstederen.

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

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

Antallet af medarbejdere, der har bemyndigelse til at udstede dokumenter med klassifikationsgraden EU TOP SECRET, skal holdes på et minimum, og deres navne skal stå på en liste, der udarbejdes af Kommissionens Sikkerhedskontor.

17.2. **Anvendelse af klassifikationsgrader**

Klassificeringen af et dokument afhænger af, hvor følsomt dets indhold er, jf. definitionen i afsnit 16. Det er vigtigt, at oplysninger klassificeres korrekt, og at der ikke anvendes en for høj klassifikationsgrad. Dette gælder navnlig anvendelse af klassifikationsgraden EU TOP SECRET.

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

En praktisk klassifikationsvejledning findes i tillæg 2.

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

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.

Retten til aktindsigt er fortsat reguleret ved forordning (EF) nr. 1049/2001.

17.3. **Nedklassificering og afklassificering**

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. Udstederen 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.

Så vidt muligt anfører udstederen på de klassificerede dokumenter en dato, periode eller begivenhed, 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.

18. FYSISK SIKKERHED

18.1. **Generelt**

Hovedformålene med fysiske sikkerhedsforanstaltninger er at forhindre uautoriseret adgang til EU-klassificerede oplysninger og/eller EU-klassificeret materiale, at forhindre tyveri og beskadigelse af udstyr og anden ejendom, og at undgå chikane og enhver anden form for forulempelse af personale, øvrige ansatte og besøgende.

18.2. **Sikkerhedskrav**

Alle lokaliteter, områder, bygninger, 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.

Når det skal afgøres, hvilken grad af fysisk sikkerhedsbeskyttelse der er nødvendig, 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 risikoen for sabotage, terrorisme, undergravende og/eller anden kriminel virksomhed.

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

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

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

c) at forhindre personer, der ikke har »need to know«-status i at få adgang til EU-klassificerede oplysninger.

18.3. **Fysiske sikkerhedsforanstaltninger**

18.3.1. *Sikkerhedszoner*

Zoner, hvor oplysninger, der er klassificeret EU CONFIDENTIAL 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 EU CONFIDENTIAL 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 med den relevante sikkerhedsgodkendelse
   iii) være forsynet med tydelig skiltning, der viser, 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 EU CONFIDENTIAL eller højere, behandles eller opbevares på en sådan måde, at medarbejdere, der ikke er berettigede til at få adgang til oplysningerne, ved hjælp af intern kontrol kan forhindres i at komme ind på områder med kontorer m.v., hvor oplysninger, der er klassificeret EU CONFIDENTIAL 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 den relevante 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.

   Zoner, hvor der ikke er vagthavende personale døgnet rundt, skal inspiceres umiddelbart efter normal arbejdstids ophør for at sikre, at EU-klassificerede oplysninger opbevares efter sikkerhedsforskrifterne.

18.3.2. *Administrativ zone*

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 sådanne zoner må der ikke behandles eller opbevares oplysninger, der er klassificeret højere end EU RESTRICTED.

18.3.3. *Adgangskontrol*

Adgang til sikkerhedszoner af klasse I og II kontrolleres ved hjælp af adgangsbadge eller et personligt identifikationssystem for alle de medarbejdere, der normalt arbejder i disse zoner. 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 fuldstændigt 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.

18.3.4. *Vagtpatruljering*

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

18.3.5. *Sikre skabe og bokse, bokslokaler m.v.*

Der anvendes tre klasser af skabe og bokse til opbevaring af EU-klassificerede oplysninger:

— Klasse A: skabe og bokse, som er godkendt til opbevaring af oplysninger, der er klassificeret EU TOP SECRET, i en sikkerhedszone af klasse I eller II

— Klasse B: skabe og bokse, som nationalt er godkendt til opbevaring af oplysninger, der er klassificeret EU SECRET eller EU CONFIDENTIAL, i en sikkerhedszone af klasse I eller II

— Klasse C: kontormøbler, hvori der ikke må opbevares oplysninger, der er klassificeret højere end EU RESTRICTED.

I bokslokaler, der er indrettet 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 EU CONFIDENTIAL eller højere, skal vægge, gulve og lofter samt dør(e) og låsemekanisme(r) være godkendt af den nationale sikkerhedsgodkendelsesmyndighed, som attesterer, at lokalerne yder samme beskyttelse som sikre skabe og bokse af den klasse, der er godkendt til opbevaring af oplysninger med samme klassifikationsgrad.

18.3.6. *Låsemekanismer*

De låsemekanismer, der anvendes til sikre skabe og bokse og bokslokaler, hvori der opbevares EU-klassificerede oplysninger, skal opfylde følgende krav:

— Gruppe A: have national godkendelse til skabe og bokse af klasse A

— Gruppe B: have national godkendelse til skabe og bokse af klasse B

— Gruppe C: må kun anvendes til kontormøbler af klasse C.

18.3.7. *Kontrol med nøgler og koder*

Nøgler til sikre skabe og bokse må ikke tages med uden for Kommissionens bygninger. Medarbejdere, der har behov for at kende koden til sikre skabe og bokse, skal lære denne udenad. Den lokale sikkerhedsansvarlige i den pågældende afdeling i Kommissionen har ansvaret for at opbevare reservenøgler samt en skriftlig fortegnelse over alle koderne, som kan anvendes, hvis der opstår en nødsituation; koderne skal opbevares hver for sig i forseglede uigennemsigtige kuverter. Arbejdsnøgler, reservesikkerhedsnøgler og koder skal opbevares i særlige sikre skabe eller bokse. Nøgler eller koder skal mindst være undergivet samme sikkerhedsbeskyttelse som det materiale, de giver adgang til.

Så få medarbejdere som muligt skal have kendskab til koderne til sikre skabe og bokse. Koderne ændres:

a) hver gang der modtages et nyt skab eller en ny boks

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) med regelmæssige mellemrum, helst hver sjette måned og mindst en gang om året.

18.3.8. *Anordninger til afsløring af uvedkommendes forsøg på at skaffe sig adgang*

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.

18.3.9. *Godkendt udstyr*

Kommissionens Sikkerhedskontor sørger for at have ajourførte fortegnelser over de typer og modeller af sikkerhedsudstyr, det har godkendt til beskyttelse af klassificerede oplysninger under forskellige nærmere angivne omstændigheder og vilkår. Kommissionens Sikkerhedskontor fører bl.a. sådanne fortegnelser på grundlag af oplysninger fra de nationale sikkerhedsmyndigheder.

18.3.10. *Fysisk beskyttelse af kopi- og telefaxmaskiner*

Kopi- og telefaxmaskiner beskyttes fysisk i det omfang, det er nødvendigt for at sikre, at kun autoriserede medarbejdere kan anvende dem til frembringelse af klassificerede oplysninger, og at alt klassificeret materiale er undergivet den fornødne kontrol.

18.4. **Beskyttelse mod uvedkommendes blikke og aflytning**

18.4.1. *Uvedkommendes blikke*

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.

18.4.2. *Aflytning*

Kontorer eller zoner, hvor der regelmæssigt drøftes anliggender, der er klassificeret EU SECRET eller højere, beskyttes mod aktiv og passiv aflytning, i det omfang en risikovurdering tilsiger det. Det påhviler Kommissionens Sikkerhedskontor at vurdere risikoen for sådan aflytning, om nødvendigt efter at have hørt nationale sikkerhedsmyndigheder.

18.4.3. *Medbringelse af elektronisk udstyr og udstyr til lydoptagelser*

Det er ikke tilladt at bringe mobiltelefoner, private computere, båndoptagere, kameraer eller andre elektroniske apparater eller andet udstyr til lydoptagelser ind i sikkerhedszoner eller teknisk sikrede zoner uden forudgående tilladelse fra chefen for Kommissionens Sikkerhedskontor.

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 der kan høres udenfor), dels aktiv aflytning (f.eks. detektion af skjulte mikrofoner), kan Kommissionens Sikkerhedskontor anmode om bistand fra de nationale sikkerhedsmyndigheder.

Når omstændighederne tilsiger det, kan sikkerhedsteknikere fra nationale sikkerhedsmyndigheder på anmodning af chefen for Kommissionens Sikkerhedskontor ligeledes inspicere telekommunikationsudstyr og det elektriske eller elektroniske kontormateriel, der anvendes under møder, hvor drøftelserne er klassificeret EU SECRET eller højere.

18.5. **Teknisk sikrede zoner**

Visse zoner kan udpeges som teknisk sikrede zoner. Der foretages en særlig adgangskontrol. Når sådanne zoner ikke bruges, skal de holdes aflåst efter en godkendt metode, 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.

Der udarbejdes en detaljeret fortegnelse over udstyr og møbler, så der kan føres kontrol med flytninger heraf. 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 detektion af aflytningsudstyr. Det er generelt ikke tilladt at installere kommunikationslinjer i teknisk sikrede zoner uden forudgående tilladelse fra den relevante myndighed.

19. ALMINDELIGE BESTEMMELSER OM »NEED-TO-KNOW«-PRINCIPPET OG PERSONLIGE EU-SIKKERHEDSGODKENDELSER

19.1. **Generelt**

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

Det påhviler den afdeling, hvor en medarbejder skal tiltræde, at afgøre, hvilke oplysninger den pågældende har tjenstligt behov for at få kendskab til.

Hver enkelt afdeling er ansvarlig for at anmode om sikkerhedsgodkendelse af medarbejderne.

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

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

Hvis det er nødvendigt at drøfte EU-klassificerede oplysninger med personer, som ikke er tjenestemænd eller andre ansatte, men f.eks. eksterne leverandører af tjenesteydelser, eksperter eller konsulenter, eller det er nødvendigt at vise dem sådanne oplysninger, skal de pågældende være personligt EU-sikkerhedsgodkendt til EU-klassificerede oplysninger, og de skal orienteres om deres sikkerhedsmæssige ansvar.

Forordning (EF) nr. 1049/2001 gælder fortsat for aktindsigt.

19.2. **Særlige bestemmelser om adgang til oplysninger, der er klassificeret EU TOP SECRET**

Enhver, der skal have adgang til oplysninger, som er klassificeret EU TOP SECRET, skal først være sikkerhedsgodkendt til denne klassifikationsgrad.

Enhver, der skal have adgang til oplysninger, som er klassificeret EU TOP SECRET, udpeges af Kommissionens medlem med ansvar for sikkerhedsspørgsmål, og deres navn optages på listen over de medarbejdere, der er sikkerhedsgodkendt til EU TOP SECRET. Kommissionens Sikkerhedskontor opretter og ajourfører denne liste.

Enhver, der skal have adgang til oplysninger, som er klassificeret EU TOP SECRET, skal forinden underskrive en erklæring om at være blevet orienteret om Kommissionens sikkerhedsprocedurer og fuldt ud at have forstået sit særlige ansvar for at beskytte oplysninger, der er klassificeret 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.

Hvis en medarbejder skal deltage i møder og lignende, hvor den pågældende vil få adgang til oplysninger, der er klassificeret EU TOP SECRET, skal den sikkerhedsansvarlige i den tjenestegren eller instans, hvor medarbejderen er ansat, meddele den instans, som afholder mødet, at medarbejderen har den nødvendige sikkerhedsgodkendelse.

Navnene på samtlige personer, hvis arbejdsopgaver ikke længere kræver adgang til oplysninger, der er klassificeret EU TOP SECRET, skal fjernes fra 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 EU TOP SECRET. De skal desuden underskrive en erklæring om, at de hverken vil bruge eller videregive oplysninger i deres besiddelse, der er klassificeret EU TOP SECRET.

19.3. **Særlige bestemmelser om adgang til oplysninger, der er klassificeret EU SECRET eller EU CONFIDENTIAL**

Enhver, der skal have adgang til oplysninger, som er klassificeret EU SECRET eller EU CONFIDENTIAL, skal først være sikkerhedsgodkendt til den pågældende klassifikationsgrad.

Enhver, der skal have adgang til oplysninger, som er klassificeret EU SECRET eller EU CONFIDENTIAL, skal gøres bekendt med de relevante sikkerhedsbestemmelser og skal være klar over konsekvenserne af uagtsomhed.

Hvis en medarbejder skal deltage i møder og lignende, hvor den pågældende vil få adgang til oplysninger, der er klassificeret EU SECRET eller EU CONFIDENTIAL, skal den sikkerhedsansvarlige i den tjenestegren eller instans, hvor medarbejderen er ansat, meddele den instans, der afholder mødet, at medarbejderen har den nødvendige sikkerhedsgodkendelse.

19.4. **Særlige bestemmelser om adgang til oplysninger, der er klassificeret EU RESTRICTED**

Enhver, der har adgang til oplysninger, som er klassificeret EU RESTRICTED, gøres bekendt med sikkerhedsbestemmelserne og konsekvenserne af uagtsomhed.

19.5. **Overdragelse af materiale**

Hvis en medarbejder skal forflyttes 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.

Hvis en medarbejder skal forflyttes til et sted, hvor der behandles EU-klassificeret materiale, orienterer den lokale sikkerhedsansvarlige vedkommende herom.

19.6. **Særlige instrukser**

Medarbejdere, som skal behandle EU-klassificerede oplysninger, bør ved tildelingen af deres arbejdsopgaver og siden med regelmæssige mellemrum gøres opmærksom på følgende:

a) sikkerhedsrisikoen ved uoverlagte ytringer

b) de forholdsregler, der skal træffes over for pressen og repræsentanter for særlige interessegrupper

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 underrette de relevante sikkerhedsmyndigheder om enhver henvendelse eller handling, der kan vække mistanke om spionage, eller enhver usædvanlig sikkerhedsrelevant omstændighed.

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, orienteres om de teknikker, sådanne efterretningstjenester vides at benytte sig af.

Kommissionen har ingen sikkerhedsbestemmelser vedrørende private rejser, som foretages af medarbejdere, der er sikkerhedsgodkendt til EU-klassificerede oplysninger. Kommissionens Sikkerhedskontor gør imidlertid medarbejderne bekendt med de rejsebestemmelser, de inden for deres ansvarsområde er omfattet af.

20. SIKKERHEDSGODKENDELSE AF KOMMISSIONENS TJENESTEMÆND OG ØVRIGE ANSATTE

a) Kun tjenestemænd og øvrige ansatte i Kommissionen eller personer, der arbejder i Kommissionen, og som i embeds medfør og af tjenstlige grunde har brug for at få kendskab til eller behandle klassificerede oplysninger i Kommissionens besiddelse, har adgang til sådanne oplysninger.

b) For at få adgang til oplysninger, der er klassificeret EU TOP SECRET, EU SECRET eller EU CONFIDENTIAL, skal de i litra a) omhandlede medarbejdere først godkendes til den pågældende klassifikationsgrad efter proceduren i litra c) og d).

c) Kun personer, der er blevet sikkerhedsundersøgt af medlemsstaternes nationale myndigheder (den nationale sikkerhedsmyndighed) efter proceduren i litra i) til n), kan godkendes.

d) Chefen for Kommissionens Sikkerhedskontor er ansvarlig for at give de godkendelser, der er nævnt i litra a), b) og c).

e) Vedkommende meddeler godkendelsen efter at have indhentet udtalelse fra medlemsstaternes nationale myndigheder på grundlag af den sikkerhedsundersøgelse, der er foretaget i henhold til litra i) til n).

f) Kommissionens Sikkerhedskontor ajourfører løbende en liste over alle følsomme stillinger, som Kommissionens afdelinger har angivet, og over alle medarbejdere, der har fået (midlertidig) godkendelse.

g) Godkendelsen, der er gyldig i fem år, må ikke være af længere varighed end de arbejdsopgaver, der ligger til grund for den. Godkendelsen kan fornys efter proceduren i litra e).

h) Chefen for Kommissionens Sikkerhedskontor kan inddrage godkendelsen, hvis vedkommende finder, at der er grund hertil. Inddrages godkendelsen, underrettes den pågældende person, der kan anmode om at måtte fremsætte sine bemærkninger over for chefen for Kommissionens Sikkerhedskontor, og de nationale myndigheder.

i) Sikkerhedsundersøgelsen foretages med den berørte persons medvirken og efter anmodning fra chefen for Kommissionens Sikkerhedskontor. Undersøgelsen foretages af myndighederne i den medlemsstat, hvor den person, der skal sikkerhedsgodkendes, er statsborger. Er den pågældende ikke statsborger i en EU-medlemsstat, anmoder chefen for Kommissionens Sikkerhedskontor den EU-medlemsstat, hvor personen har sin bopæl eller normalt opholder sig, om at foretage sikkerhedsundersøgelsen.

j) Den pågældende skal som led i sikkerhedsundersøgelsen udfylde et skema med angivelse af personlige oplysninger.

k) Chefen for Kommissionens Sikkerhedskontor giver i sin anmodning nærmere oplysninger om arten af og klassifikationsniveauet for de oplysninger, som den pågældende person vil få kendskab til, så de nationale myndigheder kan foretage sikkerhedsundersøgelsen og afgive udtalelse om, hvilket niveau den pågældende bør godkendes til.

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

m) Afgiver medlemsstaternes nationale myndigheder positiv udtalelse, kan chefen for Kommissionens Sikkerhedskontor godkende den pågældende person.

n) Afgiver de nationale myndigheder negativ udtalelse, underrettes den pågældende person, der kan anmode om at måtte fremsætte sine bemærkninger over for chefen for Kommissionens Sikkerhedskontor. Hvis chefen for Kommissionens Sikkerhedskontor finder det nødvendigt, kan vedkommende rette henvendelse til de nationale myndigheder og bede om eventuelle yderligere oplysninger. Bekræftes den negative udtalelse, kan der ikke meddeles godkendelse.

o) Enhver, der godkendes efter litra d) og e), får i forbindelse med godkendelsen og siden med jævne mellemrum de nødvendige instrukser om beskyttelse af klassificerede oplysninger og om, hvordan de skal beskyttes. Den godkendte underskriver en erklæring som bekræftelse på at have modtaget instrukserne og giver tilsagn om at overholde dem.

p) Chefen for Kommissionens Sikkerhedskontor træffer de nødvendige foranstaltninger til gennemførelse af dette afsnit, navnlig vedrørende reglerne for adgang til listen over godkendte personer.

q) Chefen for Kommissionens Sikkerhedskontor kan undtagelsesvis, hvis der er tjenstlige grunde til det, meddele midlertidig godkendelse for et tidsrum på højst seks måneder, mens resultatet af sikkerhedsundersøgelsen som omhandlet i litra i) afventes, forudsat at de nationale myndigheder på forhånd er blevet underrettet, og disse ikke har fremsat bemærkninger inden for en måned.

r) Formålsbestemte og midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret EU TOP SECRET; adgang hertil er forbeholdt tjenestemænd, som har gennemgået en egentlig sikkerhedsundersøgelse med positivt resultat efter litra i). Indtil resultatet af sikkerhedsundersøgelsen foreligger, kan tjenestemænd, for hvem der er anmodet om sikkerhedsgodkendelse til EU TOP SECRET, meddeles midlertidig og formålsbestemt godkendelse, så de kan få adgang til oplysninger, der er klassificeret til og med EU SECRET.

21. UDARBEJDELSE, FORDELING, VIDEREGIVELSE, KOPIERING, OVERSÆTTELSE OG UDDRAG AF EU-KLASSIFICEREDE DOKUMENTER OG SIKKERHEDSGODKENDELSE AF KURERPERSONALE

21.1. **Udarbejdelse**

1. EU-klassifikationsgraderne anvendes som fastsat i afsnit 16 og for EU CONFIDENTIAL eller højere og anføres centreret foroven og forneden på hver side, ligesom hver side skal forsynes med nummer. Hvert EU-klassificeret dokument skal være forsynet med referencenummer og dato. På dokumenter, der er klassificeret EU TOP SECRET eller EU SECRET, anføres referencenummeret på hver side. Hvis de skal fordeles i flere eksemplarer, skal hvert eksemplar have et nummer, som anføres på første side tillige med det samlede sideantal. På dokumenter, der er klassificeret EU CONFIDENTIAL eller højere, skal der på første side være angivet, hvor mange bilag der er.

2. Dokumenter, der er klassificeret EU CONFIDENTIAL eller højere, må kun skrives, oversættes, opbevares, fotokopieres, reproduceres magnetisk eller mikrofilmes af personer, som er blevet sikkerhedsgodkendt med henblik på adgang til EU-klassificerede oplysninger på et niveau, der mindst svarer til det pågældende dokuments klassifikationsgrad.

3. Bestemmelserne om anvendelse af PC m.v. til fremstilling af klassificerede dokumenter findes i afsnit 25.

21.2. **Fordeling**

1. EU-klassificerede oplysninger må kun komme de personer i hænde, for hvem adgang er tjenstlig nødvendig, og som har den relevante sikkerhedsgodkendelse. Dokumentets udsteder specificerer, hvem der skal modtage det.

2. Dokumenter, der er klassificeret EU TOP SECRET sendes via EU TOP SECRET-sekretariater (jf. afsnit 22.2). Når det gælder meddelelser, der er klassificeret EU TOP SECRET, kan det ansvarlige sekretariat give chefen for kommunikationscentret tilladelse til at fremstille det antal eksemplarer, som er angivet i modtagerlisten.

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

4. Ethvert dokument, der er klassificeret EU CONFIDENTIAL eller højere, skal, når det ankommer til eller forlader et generaldirektorat eller en tjenestegren, registreres af det lokale sekretariat for EU-klassificerede oplysninger. 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 (jf. afsnit 22.1).

21.3. **Videregivelse af EU-klassificerede dokumenter**

21.3.1. *Emballering og kvitteringer*

1. Dokumenter, der er klassificeret EU CONFIDENTIAL 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.

2. Kun en sikkerhedsansvarlig for et sekretariat (jf. afsnit 22.1)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 (jf. afsnit 22.1), og kun den person, den er adresseret til, må åbne den inderste kuvert og kvittere for modtagelsen af de fremsendte dokumenter.

3. 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.

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

5. Når det drejer sig om dokumenter, der er klassificeret EU CONFIDENTIAL eller højere, modtager kureren en kvittering for hvert registreringsnummer.

21.3.2. *Videregivelse inden for en bygning eller gruppe af bygninger*

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

21.3.3. *Videregivelse inden for et lands grænser*

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

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

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

   a) bæreren af dokumentet skal være sikkerhedsgodkendt til EU TOP SECRET-dokumenter

   b) transportmåden skal være i overensstemmelse med reglerne om videregivelse af EU TOP SECRET-dokumenter

   c) medarbejderen må under ingen omstændigheder efterlade EU TOP SECRET-dokumentet uden opsyn

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

4. Inden for et givet lands grænser kan dokumenter, der er klassificeret EU SECRET eller EU CONFIDENTIAL, 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 EU-klassificerede oplysninger.

5. Kommissionens Sikkerhedskontor udarbejder på grundlag af disse bestemmelser instrukser om personlig transport af EU-klassificerede dokumenter. Bæreren af dokumenterne 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 18

   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.

21.3.4. *Videregivelse fra en stat til en anden*

1. Materiale, der er klassificeret EU CONFIDENTIAL eller højere, sendes med EU-diplomatpost eller militær kurertjeneste.

2. Der kan imidlertid gives tilladelse til personlig transport af materiale, der er klassificeret EU SECRET eller EU CONFIDENTIAL, hvis materialet transporteres på en sådan måde, at det ikke kan komme uvedkommende i hænde.

3. Kommissionens medlem med ansvar for sikkerhedsspørgsmål kan give tilladelse til personlig transport, hvis der ikke er mulighed for at anvende diplomatpost eller militær kurertjeneste, eller hvis anvendelse heraf vil medføre en forsinkelse, der vil skade EU's operationer, og det haster med at få materialet frem til modtageren. Kommissionens Sikkerhedskontor udarbejder instrukser om anden form for international personlig transport af materiale med klassifikationsgrad til og med EU SECRET end diplomatpost og militær kurertjeneste. Instrukserne skal indeholde følgende krav:

   a) bæreren af materialet skal være sikkerhedsgodkendt til den pågældende klassifikationsgrad

   b) alt, hvad der transporteres på denne måde, skal registreres af vedkommende afdeling eller 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) bæreren skal være i besiddelse af et kurercertifikat og/eller en tjenesterejseordre, som er anerkendt af alle EU-medlemsstater og giver tilladelse til at transportere pakken som beskrevet

   e) bæreren må ved rejse over land ikke 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) bærerens rejseplaner med hensyn til bestemmelsessted, rejseruter og 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 bærerens varetægt, medmindre det deponeres i overensstemmelse med bestemmelserne om deponering i afsnit 18

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).

4. 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.

21.3.5. *Videregivelse af dokumenter klassificeret EU RESTRICTED*

Der er ikke fastsat særlige bestemmelser for forsendelse af dokumenter, der er klassificeret EU RESTRICTED, men det skal dog sikres, at uvedkommende ikke kommer i besiddelse af dem.

21.4. **Sikkerhedsgodkendelse af kurerpersonale**

Alle kurerer, der ansættes til at transportere dokumenter, der er klassificeret EU SECRET eller EU CONFIDENTIAL, skal forinden have den relevante sikkerhedsgodkendelse.

21.5. **Elektronisk eller anden teknisk videregivelse**

1. Der træffes foranstaltninger med hensyn til kommunikationssikkerhed, så EU-klassificerede oplysninger kan videregives under sikre forhold. De nærmere bestemmelser om videregivelse af EU-klassificerede oplysninger er omhandlet i afsnit 25.

2. Oplysninger, der er klassificeret EU CONFIDENTIAL eller EU SECRET, må kun videregives via godkendte kommunikationscentre og -netværk og/eller godkendte terminaler og systemer.

21.6. **Kopiering, oversættelse og uddrag af EU-klassificerede dokumenter**

1. Dokumenter, der er klassificeret EU TOP SECRET, må kun kopieres eller oversættes med udstederens godkendelse.

2. Hvis medarbejdere, der ikke er sikkerhedsgodkendt til EU TOP SECRET, har brug for oplysninger, som er indeholdt i et EU TOP SECRET-dokument, men ikke er klassificeret så højt, kan lederen af EU TOP SECRET-sekretariatet (jf. afsnit 22.2) bemyndiges 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.

3. Dokumenter, der er klassificeret EU SECRET eller lavere, kan mangfoldiggøres og oversættes af modtageren inden for rammerne af sikkerhedsbestemmelserne, for så vidt det sker under nøje overholdelse af »need-to-know«-princippet. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, gælder også for kopier og/eller oversættelser af det.

22. SEKRETARIATER FOR EU-KLASSIFICEREDE OPLYSNINGER, KONTROL, ARKIVERING OG DESTRUKTION AF EU-KLASSIFICEREDE OPLYSNINGER

22.1. **Lokale sekretariater for EU-klassificerede oplysninger**

1. I Kommissionen, eventuelt i hver enkelt afdeling, er et eller flere lokale sekretariater for EU-klassificerede oplysninger ansvarlige for registrering, reproduktion, forsendelse, arkivering og destruktion af dokumenter, der er klassificeret EU SECRET eller EU CONFIDENTIAL.

2. Hvis en afdeling ikke har et lokalt sekretariat for EU-klassificerede oplysninger, varetager Generalsekretariatets lokale sekretariat for EU-klassificerede oplysninger denne funktion.

3. De lokale sekretariater for EU-klassificerede oplysninger refererer til lederen af den afdeling, som de modtager deres instrukser fra. Sekretariatslederne er sikkerhedsansvarlige.

4. De hører ind under den lokale sikkerhedsansvarlige med hensyn til anvendelse af bestemmelserne om håndtering af EU-klassificerede dokumenter og overholdelse af de tilsvarende sikkerhedsforanstaltninger.

5. Medarbejdere, der udpeges til de lokale sekretariater for EU-klassificerede dokumenter, skal være sikkerhedsgodkendt til EU-klassificerede dokumenter, jf. afsnit 20.

6. De lokale sekretariater for EU-klassificerede dokumenter udfører følgende opgaver under den relevante afdelingsleders ansvar:

   a) administrerer arbejdet med registrering, reproduktion, oversættelse, videregivelse, forsendelse og destruktion af oplysningerne

   b) ajourfører listen over data vedrørende klassificerede oplysninger

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

7. De lokale sekretariater for EU-klassificerede oplysninger fører et register, der omfatter følgende data:

   a) dato for udarbejdelsen af de klassificerede oplysninger

   b) klassifikationsgrad

   c) den dato, indtil hvilken oplysningerne er klassificeret

   d) udstederens navn og afdeling

   e) modtageren eller modtagerne med angivelse af løbenummer

   f) emne

   g) nummer

   h) antal videregivne eksemplarer

   i) opgørelser over, hvilke klassificerede oplysninger der er leveret til afdelingen

   j) registrering af afklassificering og nedklassificering af klassificerede oplysninger.

8. De almindelige bestemmelser i afsnit 21 gælder for Kommissionens lokale sekretariater for EU-klassificerede oplysninger, medmindre de særlige bestemmelser i dette afsnit afviger herfra.

22.2. **EU TOP SECRET-sekretariatet**

22.2.1. *Generelt*

1. Et centralt EU TOP SECRET-sekretariat varetager registreringen, håndteringen og fordelingen af EU TOP SECRET-dokumenter i henhold til disse sikkerhedsbestemmelser. Lederen af EU TOP SECRET-sekretariatet er sikkerhedsansvarlig for EU TOP SECRET-sekretariatet.

2. Det centrale EU TOP SECRET-sekretariat fungerer som Kommissionens øverste modtagelses- og afsendelsesmyndighed over for de andre EU-institutioner, medlemsstaterne, internationale organisationer og tredjelande, med hvilke Kommissionen har sikkerhedsaftaler om udveksling af klassificerede oplysninger.

3. Om nødvendigt oprettes der undersekretariater med ansvar for den interne styring af dokumenter, der er klassificeret 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 22.2.3 EU TOP SECRET-undersekretariater, som tilknyttes et centralt EU TOP SECRET-sekretariat. Hvis der kun midlertidigt og lejlighedsvis er behov for at konsultere dokumenter, der er klassificeret EU TOP SECRET, kan sådanne dokumenter fordeles, uden at der oprettes et EU TOP SECRET-undersekretariat, hvis der fastsættes regler for at sikre, at det pågældende EU TOP SECRET-sekretariat bevarer kontrollen med dokumenterne, og at samtlige fysiske og personalemæssige sikkerhedsforanstaltninger overholdes.

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

6. Al udveksling af dokumenter, der er klassificeret EU TOP SECRET, mellem undersekretariater, som ikke er tilknyttet samme centrale sekretariat, skal foregå via de centrale EU TOP SECRET-sekretariater.

22.2.2. *Det centrale EU TOP SECRET-sekretariat*

Som sikkerhedsansvarlig er lederen af det centrale EU TOP SECRET-sekretariat ansvarlig for:

a) at dokumenter, der er klassificeret EU TOP SECRET, videregives i overensstemmelse med bestemmelserne i afsnit 21.3

b) at der løbende ajourføres en liste over samtlige EU TOP SECRET-undersekretariater, der er tilknyttet sekretariatet, samt en liste over de udpegede sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift

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

d) at der føres et register over opbevarede og fordelte EU TOP SECRET-dokumenter

e) at der løbende ajourføres en liste over alle de centrale EU TOP SECRET-sekretariater, som vedkommende jævnligt er i forbindelse med, tillige med de udpegede sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift

f) at alle sekretariatets dokumenter, der er klassificeret EU TOP SECRET, opbevares fysisk sikkert i overensstemmelse med bestemmelserne i afsnit 18.

22.2.3. *EU TOP SECRET-undersekretariater*

Som sikkerhedsansvarlig er lederen af et EU TOP SECRET-undersekretariat ansvarlig for:

a) at dokumenter, der er klassificeret EU TOP SECRET, videregives i overensstemmelse med bestemmelserne i afsnit 21.3

b) at der løbende ajourføres en liste over alle, der har adgang til de EU TOP SECRET-oplysninger, der er i vedkommendes varetægt

c) at dokumenter, der er klassificeret 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 der løbende ajourføres et register over alle dokumenter, der er klassificeret EU TOP SECRET, og som opbevares og fordeles under vedkommendes kontrol, eller som er overført til andre EU TOP SECRET-sekretariater, og at samtlige kvitteringer i forbindelse hermed opbevares

e) at der løbende ajourføres en liste over de EU TOP SECRET-sekretariater, som vedkommende har bemyndigelse til at udveksle EU TOP SECRET-dokumenter med, tillige med de sikkerhedsansvarliges og deres bemyndigede stedfortræderes navn og underskrift

f) at alle undersekretariatets dokumenter, der er klassificeret EU TOP SECRET, opbevares fysisk sikkert i overensstemmelse med bestemmelserne i afsnit 18.

22.3. **Opgørelser over og kontrol af EU-klassificerede dokumenter**

1. Hvert år udarbejder hvert EU TOP SECRET-sekretariat som nævnt i dette afsnit en specificeret opgørelse over alle EU TOP SECRET-dokumenter. Sekretariatet anses for at have redegjort for et dokument, hvis det fysisk er i besiddelse af dokumentet eller af en kvittering fra det EU TOP SECRET-sekretariat, hvortil dokumentet er blevet sendt, en destruktionsattest for det pågældende dokument eller en instruks om at nedklassificere eller afklassificere det. De sender resultatet af deres årsopgørelse til Kommissionens medlem med ansvar for sikkerhedsspørgsmål senest den 1. april hvert år.

2. EU TOP SECRET-undersekretariaterne sender resultatet af deres årsopgørelse til det centrale sekretariat, som de sorterer under, på en dato, som fastsættes af det centrale sekretariat.

3. EU-klassificerede dokumenter med en klassifikationsgrad, der er lavere end EU TOP SECRET, underkastes intern kontrol i overensstemmelse med instrukser fra Kommissionens medlem med ansvar for sikkerhedsspørgsmål.

4. Alt dette giver mulighed for at danne sig et billede af, hvilke dokumenter der ifølge ihændehaverne kan:

   a) nedklassificeres eller afklassificeres

   b) destrueres.

22.4. **Arkivering af EU-klassificerede oplysninger**

1. EU-klassificerede oplysninger opbevares under forhold, der er i overensstemmelse med kravene i afsnit 18.

2. For at begrænse opbevaringsproblemerne mest muligt har de sikkerhedsansvarlige for alle sekretariater bemyndigelse til at lade dokumenter, der er klassificeret EU TOP SECRET, EU SECRET eller EU CONFIDENTIAL, mikrofilme eller på anden måde arkivere i en magnetisk eller optisk udgave på følgende betingelser:

   a) optagelsen på mikrofilm/arkiveringen 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 originale dokumenter

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

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

   e) optagelse/arkivering af et dokument, der er klassificeret EU TOP SECRET eller EU SECRET, angives tydeligt i det register, der anvendes til årsopgørelsen

   f) originale dokumenter, som er blevet mikrofilmet, eller som opbevares på anden vis, destrueres i overensstemmelse med bestemmelserne i afsnit 22.5.

3. Disse bestemmelser gælder ligeledes for andre former for godkendt opbevaring, såsom elektromagnetiske og optiske medier.

22.5. **Destruktion af EU-klassificerede dokumenter**

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

   a) dokumenter, der er klassificeret EU TOP SECRET, må kun destrueres af det centrale sekretariat, som er ansvarligt for dem. Hvert af de destruerede dokumenter anføres i en destruktionsattest, som underskrives af den sikkerhedsansvarlige på EU TOP SECRET-niveau og af den medarbejder, der overværer destruktionen, og som skal være sikkerhedsgodkendt til EU TOP SECRET. Der indføres en bemærkning herom i journalen

   b) sekretariatet opbevarer destruktionsattester og fortegnelser over fordeling i ti år. Der sendes kun kopier til udstederen eller det relevante centrale sekretariat på udtrykkelig anmodning

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

2. Dokumenter, der er klassificeret EU SECRET, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, under opsyn af en sikkerhedsgodkendt medarbejder og ved hjælp af en af processerne i nr. 1, litra c). Destruerede dokumenter, der var klassificeret EU SECRET, anføres på underskrevne destruktionsattester, som sekretariatet opbevarer i mindst tre år tillige med fortegnelser over udbredelse.

3. Dokumenter, der er klassificeret EU CONFIDENTIAL, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, under opsyn af en sikkerhedsgodkendt medarbejder og ved hjælp af en af processerne i nr. 1, litra c). Destruktionen af dem registreres i overensstemmelse med instrukser fra Kommissionens medlem med ansvar for sikkerhedsspørgsmål.

4. Dokumenter, der er klassificeret EU RESTRICTED, destrueres af det sekretariat, som er ansvarligt for de pågældende dokumenter, eller af brugeren i overensstemmelse med instrukser fra Kommissionens medlem med ansvar for sikkerhedsspørgsmål.

22.6. **Destruktion i krisesituationer**

1. Kommissionens afdelinger udarbejder på grundlag af lokale forhold planer for sikker opbevaring af EU-klassificeret materiale i krisesituationer, herunder om nødvendigt planer for destruktion eller flytning. Den bekendtgør de instrukser, som den finder nødvendige for at undgå, uvedkommende får EU-klassificerede oplysninger i hænde.

2. Foranstaltningerne til sikker opbevaring og/eller destruktion i krisesituationer af materiale, der er klassificeret EU SECRET eller EU CONFIDENTIAL, må under ingen omstændigheder være til skade for opbevaringen eller destruktionen af materiale, der er klassificeret EU TOP SECRET; dette gælder ligeledes krypteringsudstyr, som skal prioriteres over alt andet.

3. Der udstedes særlige instrukser vedrørende foranstaltninger til sikker opbevaring og destruktion af krypteringsudstyr i en krisesituation.

4. Instrukserne skal opbevares på stedet i en lukket kuvert. Der skal være midler/værktøj til destruktion til rådighed.

23. SIKKERHEDSFORANSTALTNINGER FOR SÆRLIGE MØDER AFHOLDT UDEN FOR KOMMISSIONENS LOKALER OG MED INDDRAGELSE AF KLASSIFICEREDE OPLYSNINGER

23.1. **Generelt**

Hvis møder i Kommissionen eller andre vigtige møder ikke afholdes i Kommissionens lokaler, 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.

23.2. **Ansvarsopgaver**

23.2.1. *Kommissionens Sikkerhedskontor*

Kommissionens Sikkerhedskontor skal samarbejde med de kompetente myndigheder i den medlemsstat, på hvis territorium mødet afholdes (værtslandet), med henblik på at garantere Kommissionens eller andre vigtige møders sikkerhed og af hensyn til de delegeredes og deres medarbejderes 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 Kommissionens kommunikationssystem med henblik på modtagelse og videregivelse af EU-klassificerede oplysninger. Værtslandet anmodes om i nødvendigt omfang at stille sikrede telefonsystemer til rådighed.

Kommissionens Sikkerhedskontor fungerer som sikkerhedsrådgiver under forberedelsen af møderne; det sender en repræsentant til stedet til at assistere og rådgive den sikkerhedsansvarlige for mødet og delegationerne.

Hver af delegationerne udpeger en sikkerhedsansvarlig, som har ansvaret for sikkerhedsspørgsmål i den pågældende delegation og for at opretholde den fornødne kontakt med den sikkerhedsansvarlige for møderne og med Kommissionens Sikkerhedskontor.

23.2.2. *Sikkerhedsansvarlig for møder*

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

a) 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

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

c) løbende samordning med værtsmedlemslandets kompetente myndigheder og Kommissionens sikkerhedskontor

d) indsættelse af et eksemplar af sikkerhedsinstrukserne i hvert dokument-charteque til mødet under hensyn til kravene i disse sikkerhedsforskrifter og alle andre sikkerhedsinstrukser, som måtte findes relevante.

23.3. **Sikkerhedsforanstaltninger**

23.3.1. *Sikkerhedszoner*

Der oprettes følgende sikkerhedszoner:

a) Sikkerhedszone af klasse II, bestående af arbejdsrum, Kommissionens kontorer og reprografisk udstyr samt delegationskontorer, hvis dette er relevant

b) Sikkerhedszone af klasse I, bestående af mødelokalet med kabiner 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.

23.3.2. *Adgangsbadger*

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

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

Ud over deltagere med adgangsbadge skal så få som muligt have adgang til mødelokaliteterne. Den sikkerhedsansvarlige for mødet giver kun nationale delegationer tilladelse til at modtage besøgende under mødet efter anmodning. Besøgende får udleveret et gæstekort. Der skal udfyldes en formular for besøgende med angivelse af den besøgendes navn og navnet på den person, som modtager besøg. Besøgende skal under hele besøget ledsages af en sikkerhedsvagt eller den person, som modtager besøg. Ovennævnte formular medbringes af den person, der ledsager den besøgende, og leveres tilbage til sikkerhedspersonalet sammen med gæstebadgen, når den besøgende forlader mødelokaliteterne.

23.3.3. *Kontrol af foto- og andet optageudstyr*

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.

23.3.4. *Undersøgelse af dokumentmapper, bærbare computere og pakker*

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 sikkerhedsansvarlige, gennemlyses med særligt udstyr eller åbnes af sikkerhedspersonalet med henblik på nærmere undersøgelse. Hvis den sikkerhedsansvarlige for mødet finder det nødvendigt, kan der træffes skærpede kontrolforanstaltninger for undersøgelse af dokumentmapper og pakker.

23.3.5. *Teknisk sikkerhed*

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

23.3.6. *Dokumenter i delegationernes varetægt*

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 værtsmedlemslandet til transport af klassificerede dokumenter til og fra mødelokaliteterne.

23.3.7. *Sikker opbevaring af dokumenter*

Hvis 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 den sikkerhedsansvarlige for mødet, som derefter opbevarer dokumenterne i overensstemmelse med godkendte normer.

23.3.8. *Kontoreftersyn*

Den sikkerhedsansvarlige for mødet drager omsorg for, at Kommissionen 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.

23.3.9. *Bortskaffelse af EU-klassificeret affald*

Alt affald behandles som EU-klassificeret, og papirkurve og affaldsposer afleveres til Kommissionen og delegationerne med henblik på bortskaffelse. Inden Kommissionen og delegationerne forlader de lokaler, som de har fået tildelt, afleverer de deres affald til den sikkerhedsansvarlige for mødet, som sørger for, at det destrueres efter gældende bestemmelser.

Ved mødets afslutning behandles samtlige dokumenter, som Kommissionen eller delegationerne er i besiddelse af, men ikke længere har brug for, som affald. Der foretages en grundig gennemsøgning af de lokaler, som Kommissionen 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 22.5.

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

24.1. **Definitioner**

Brud på sikkerhedsbestemmelserne er en handling eller forsømmelse, hvorved Kommissionens sikkerhedsbestemmelser overtrædes, og EU-klassificerede oplysninger ikke længere er sikrede og risikerer at lække.

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.

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.

24.2. **Indberetning af brud på sikkerheden**

Enhver, som skal håndtere EU-klassificerede oplysninger, skal grundigt orienteres om deres ansvar i den forbindelse. Ved ethvert brud på sikkerheden, som de får kendskab til, skal de straks indberette dette.

Opdager en lokal sikkerhedsansvarlig eller en sikkerhedsansvarlig for et møde eller underrettes en sådan sikkerhedsansvarlig om, at der er sket et brud på sikkerhedsbeskyttelsen af EU-klassificerede oplysninger, eller at EU-klassificeret materiale er gået tabt eller forsvundet, skal den pågældende træffe de fornødne foranstaltninger for at

a) sikre bevismateriale

b) redegøre for de faktiske hændelser

c) vurdere og begrænse den forvoldte skade

d) forhindre en gentagelse

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

I den forbindelse skal følgende oplysninger meddeles:

i) en beskrivelse af arten af de pågældende klassificerede oplysninger, herunder klassifikationsgrad, reference- 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.

Sikkerhedsmyndighederne har pligt til, når et brud på sikkerhedsbestemmelserne er indberettet, straks at give meddelelse herom til Kommissionens Sikkerhedskontor.

Vedrører hændelsen oplysninger, der er klassificeret EU RESTRICTED, rapporteres kun, hvis der foreligger usædvanlige omstændigheder.

Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål 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.

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

24.3. **Retlige foranstaltninger**

Enhver, der har ansvaret for lækage af EU-klassificerede oplysninger, pålægges disciplinære sanktioner i henhold til de relevante regler og bestemmelser, navnlig afsnit VI i personalevedtægten. Disciplinære sanktioner udelukker ikke, at der træffes yderligere retlige foranstaltninger.

Om nødvendigt skal Kommissionens medlem med ansvar for sikkerhedsspørgsmål på grundlag af den i afsnit 24.2, nævnte rapport tage de nødvendige skridt for at sikre, at de nationale myndigheder kan indlede strafferetlig forfølgning.

25. BESKYTTELSE AF EU-KLASSIFICEREDE OPLYSNINGER VED BRUG AF INFORMATIONSTEKNOLOGI OG KOMMUNIKATIONSSYSTEMER

25.1. **Indledning**

25.1.1. *Generelt*

Sikkerhedspolitikken og -kravene gælder for alle kommunikations- og informationssystemer og net (i det følgende benævnt »systemer«), som behandler oplysninger, der er klassificeret EU CONFIDENTIAL eller højere. De skal anvendes som supplement til Kommissionens afgørelse K(95) 1510 endelig udg. af 23. november 1995 om beskyttelse af edb-systemer.

Systemer, som behandler oplysninger, der er klassificeret EU RESTRICTED, 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.

Kommissionens IT-sikkerhedspolitik omfatter følgende:

— Den indgår som en integreret del af sikkerheden generelt og supplerer i enhver sammenhæng informationssikkerheden, personsikkerheden og den fysiske sikkerhed.

— En ansvarsdeling mellem de tekniske systemers driftsmyndigheder, ejere af de EU-klassificerede oplysninger, der er lagret, eller som behandles i systemerne, IT-sikkerhedsspecialister og brugere.

— En beskrivelse af sikkerhedsprincipperne og kravene til hvert enkelt IT-system.

— Godkendelse af disse principper og krav ved en hertil udpeget myndighed.

— Hensyntagen til de særlige trusler og sårbarheden på IT-området.

25.1.2. *Trusler mod systemer og deres sårbarhed*

En trussel kan 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, går tabt. Sårbarhed kan defineres som en svaghed eller utilstrækkelig kontrol, som vil lette eller tillade, at en trussel aktiveres mod et specifikt aktiv eller mål.

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 trusler. 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.

25.1.3. *Hovedformålet med sikkerhedsforanstaltninger*

Hovedformålet med de sikkerhedsforanstaltninger, der er omhandlet i dette afsnit, er at beskytte EU-klassificerede oplysninger mod uautoriseret indsigt (tab af fortrolighed) 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 Kommissionens Sikkerhedskontor specificere de relevante normer for konventionel sikkerhed tillige med passende specifikke sikkerhedsprocedurer og -teknikker, der er tilpasset det enkelte system.

25.1.4. *Systemspecifikke sikkerhedskrav*

For alle systemer, der behandler oplysninger klassificeret som EU CONFIDENTIAL eller højere, stilles en række systemspecifikke sikkerhedskrav, der skal formuleres af det tekniske systems driftsmyndighed (jf. afsnit 25.3.4) og ejeren af oplysningerne (jf. afsnit 25.3.5), med indlæsning og nødvendig assistance fra projektpersonalet og Kommissionens sikkerhedsansvarlige (Infosec-myndighed — IA, jf. afsnit 25.3.3) og godkendes af sikkerhedsgodkendelsesmyndigheden (jf. afsnit 25.3.2).

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

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.

25.1.5. *Sikkerhedsdriftsformer*

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

a) dedicated

b) system high

c) multi-level

25.2. **Definitioner**

Ved »godkendelse« forstås: tilladelse til og godkendelse af et system til at behandle EU-klassificerede oplysninger i dets operationelle miljø.

Bemærk:

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 imødegåelse heraf

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.

Ved »central sikkerhedsansvarlig for oplysninger« (CISO) forstås en tjenestemand i en central IT-afdeling, som koordinerer og overvåger sikkerhedsforanstaltninger for centralt styrede systemer.

Ved »certificering« forstås: udstedelse af en formel erklæring, der støttes af en uafhængig gennemgang af gennemførelsen og resultaterne af en evaluering, om i hvilket omfang et system opfylder sikkerhedskravet eller et computersikkerhedsprodukt opfylder forudfastlagte sikkerhedskrav.

Ved »kommunikationssikkerhed« (COMSEC) forstås: anvendelse af sikkerhedsforanstaltninger på telekommunikation, så uautoriserede personer ikke har adgang til oplysninger af værdi, der kan indhentes, hvis man er i besiddelse af eller har studeret telekommunikationsudstyr, eller for at sikre pålideligheden af telekommunikation.

Bemærk:

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

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.

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.

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.

Bemærk:

(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 systemet.

(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.

Ved »evaluering« forstås: vedkommende myndigheds detaljerede tekniske gennemgang af et system eller af et kryptografisk eller et computersikkerhedsprodukts sikkerhedsaspekter.

Bemærk:

(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.

Ved »ejer af oplysningerne« (IO) forstås den myndighed (direktør), som har ansvaret for udarbejdelse, behandling og anvendelse af oplysninger, inkl. ansvaret for at afgøre, hvem der skal have adgang til oplysningerne.

Ved »informationssikkerhed« (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 indgreb 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.

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

Bemærk:

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

Ved »IT-net« 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.

Bemærk:

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

(2) Et IT-net kaldes »lokalt«, hvis det forbinder flere computere sammen på samme lokalitet.

Ved »IT-netfeatures« 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 brugerne), og som er nødvendige for at sikre en acceptabel beskyttelsesgrad for klassificerede oplysninger.

Ved »IT-system« forstås: en samling af udstyr, metoder og procedurer samt eventuelt nødvendigt personale med henblik på at udføre databehandlingsfunktioner.

Bemærk:

(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 IT-systemdriftsmyndighed.

(4) Et IT-system kan indeholde undersystemer, hvoraf nogle selv er IT-systemer.

»IT-systemsikkerhedsfeatures« omfatter alle hardware-, firmware- og softwarefunktioner, karakteristika og features; drifts- og ansvarsprocedurer samt adgangskontrol, IT-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 IT-system.

Ved »lokal edb-sikkerhedsansvarlig« (LISO) forstås en tjenestemand i Kommissionen, som er ansvarlig for koordinering og overvågning af sikkerhedsforanstaltninger inden for sit område.

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.

Bemærk:

(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 sikre selektiv adgang til og adskillelse af forskellige oplysninger inden for systemet.

Ved »fjernterminal/arbejdsstationsområdet« forstås: et område med computerudstyr med tilhørende lokale ydre komponenter eller terminaler/arbejdsstationer og alt forbundet kommunikationsudstyr, som er adskilt fra et IT-område.

Ved »sikkerhedsdriftsprocedurer« forstås procedurer udarbejdet af de tekniske systemers driftsmyndighed med en definition af de principper, der skal vedtages i sikkerhedssammenhæng, de driftsprocedurer, der skal følges, og personalets ansvar.

Ved »system-high-sikkerhedsdriftsform« forstås: en driftsform, hvor ALLE personer, der har adgang til systemet, er godkendt til den højeste klassifikationsgrad for de oplysninger, der behandles inden for systemet, men 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.

Bemærk:

(1) En ikke-generel »need-to-know«-status forudsætter, at de pågældende sikkerhedsfeatures sikrer en selektiv adgang til og adskillelse af oplysningerne inden for systemet.

(2) Andre sikkerhedsfeatures (vedrørende f.eks. fysisk sikring, personale og procedurer) skal være i overensstemmelse med kravene til den højeste klassifikationsgrad og alle kategoriangivelser for de 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.

»De systemspecifikke sikkerhedskrav« (SSRS) 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 Kommissionens 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 den projektdokumentation, der skal forelægges for vedkommende myndigheder med henblik på teknisk, budgetmæssig og sikkerhedsmæssig godkendelse. I den endelige form udgør de systemspecifikke sikkerhedskrav en fuldstændig specifikation af systemets sikkerhed.

Ved »det tekniske systems driftsmyndighed« (TSO) forstås den myndighed, der har ansvaret for oprettelse, vedligeholdelse, drift og nedlukning af et system.

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

25.3. **Sikkerhedsansvar**

25.3.1. *Generelt*

Kommissionens rådgivende gruppe for sikkerhedspolitik (defineret i afsnit 12) har blandt sine ansvarsområder bl.a. INFOSEC-emner. Sikkerhedsgruppen tilrettelægger sine aktiviteter på en sådan måde, at den kan stille ekspertrådgivning til rådighed om ovennævnte spørgsmål.

Kommissionens Sikkerhedskontor er ansvarlig for udarbejdelsen af detaljerede INFOSEC-bestemmelser baseret på bestemmelserne i dette kapital.

Opstår der problemer vedrørende sikkerhedsbeskyttelsen (uheld, brud på sikkerhedsbestemmelserne m.v.) skal Kommissionens Sikkerhedskontor øjeblikkeligt gribe ind.

Der skal i Kommissionens Sikkerhedskontor være en INFOSEC-afdeling.

25.3.2. *Sikkerhedsgodkendelsesmyndighed (SAA)*

Lederen af Kommissionens Sikkerhedskontor er Kommissionens sikkerhedsgodkendelsesmyndighed (SAA). Sikkerhedsgodkendelsesmyndigheden har ansvaret inden for det generelle sikkerhedsområde og inden for specielle områder som INFOSEC, kommunikationssikkerhed, kryptografisk sikkerhed og Tempest-sikkerhed.

Sikkerhedsgodkendelsesmyndigheden er ansvarlig for at sikre systemernes overensstemmelse med Kommissionens sikkerhedspolitik. En af dens opgaver er at godkende systemer, der skal behandle EU-klassificerede oplysninger med en bestemt klassifikationsgrad i operationelle miljøer.

Jurisdiktionen for Kommissionens sikkerhedsgodkendelsesmyndighed omfatter alle de systemer, der er i drift inden for Kommissionens bygninger. Kommer forskellige komponenter i et system ind under både Kommissionens sikkerhedsgodkendelsesmyndigheds og andre sikkerhedsgodkendelsesmyndigheders jurisdiktion, udpeger parterne en fælles godkendelsesbestyrelse, idet Kommissionens sikkerhedsgodkendelsesmyndighed står for samordningen.

25.3.3. *INFOSEC-myndigheden (IA)*

Lederen af INFOSEC-afdelingen i Kommissionens Sikkerhedskontor er Kommissionens INFOSEC-myndighed. INFOSEC-myndigheden har ansvaret 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.

25.3.4. *De tekniske systemers driftsmyndighed (TSO)*

Det er driftsmyndigheden, dvs. det tekniske systems driftsmyndighed (TSO), der har ansvaret for gennemførelse og drift af kontrol- og særlige sikkerhedsfeatures i forbindelse med et givet system. I forbindelse med centralt ejede systemer udnævnes der en central edb-sikkerhedsansvarlig (CISO). Hver afdeling udnævner, hvis det er relevant, en lokal edb-sikkerhedsansvarlig (LISO). Det tekniske systems driftsmyndighed er ansvarlig for udarbejdelsen af sikkerhedsdriftsprocedurer, og dette ansvar gælder under hele et systems livscyklus fra et projekts planlægningsstadium til afslutning.

Det tekniske systems driftsmyndighed specificerer sikkerhedsstandarder og sikkerhedspraksis, der skal opfyldes af leverandøren af systemet.

Det tekniske systems driftsmyndighed kan eventuelt delegere en del af sit ansvar til en lokal edb-sikkerhedsansvarlig. De forskellige INFOSEC-funktioner kan samles hos en enkelt person.

25.3.5. *Ejeren af oplysninger (IO)*

Ejeren af oplysninger er ansvarlig for EU-klassificerede oplysninger (og andre oplysninger), som skal indføres, behandles og fremstilles i tekniske systemer. Han opstiller adgangskravene til disse oplysninger i tekniske systemer. Ansvaret herfor kan delegeres til en Information Manager eller en Database Manager inden for den ansvarliges område.

25.3.6. *Brugere*

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

25.3.7. *INFOSEC-uddannelse*

Alle ansatte, som har brug for det, skal have adgang til INFOSEC-uddannelse.

25.4. **Ikke-tekniske sikkerhedsforanstaltninger**

25.4.1. *Sikkerheden og medarbejderne*

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 Kommissionens procedurer.

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

Systemerne specificeres og udformes på en måde, der letter tildelingen af pligter og ansvar til medarbejderne, således at en enkelt medarbejder ikke får fuldstændigt kendskab til eller kontrol med sikkerhedssystemets nøglepunkter.

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

Et systems sikkerhedsfeatures må kun ændres af to ansatte, som har beføjelse hertil, og som arbejder sammen.

25.4.2. *Fysisk sikkerhed*

Informationsteknologiområder eller områder med fjernterminal/arbejdsstation (som defineret i afsnit 25.2), hvor oplysninger, der er klassificeret EU CONFIDENTIAL eller højere, behandles ved hjælp af IT-redskaber, eller hvor potentiel adgang til sådanne oplysninger ikke kan udelukkes, skal erklæres EU Klasse I- eller Klasse II-sikkerhedsområder.

25.4.3. *Kontrol af adgang til et system*

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.

Adgangskontroldata og -materiel destrueres som omhandlet i afsnit 25.5.4, hvis sådanne data eller sådant materiel ikke mere anvendes til dette formål.

25.5. **Tekniske sikkerhedsforanstaltninger**

25.5.1. *Sikkerhedsbeskyttelse af oplysninger*

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.

Det påhviler Kommissionens tjenestegrene og deres informationsihændehavere 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.

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.

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.

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.

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 af sikkerhedsgodkendelsesmyndigheden godkendt procedure (jf. 25.5.4).

25.5.2. *Kontrol med og ansvar for adgang til oplysninger*

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

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.

Opnås udskrivningerne fra et system, der behandler EU-klassificerede oplysninger, og videregives oplysningerne til et område med fjernterminalarbejdsstation fra et informationsteknologi-område, fastsættes der procedurer, der skal være godkendt af sikkerhedsgodkendelsesmyndigheden, med henblik på kontrol af fjernudskrivningen. For klassifikationsgraden EU SECRET eller højere skal sådanne procedurer omfatte specifikke instrukser vedrørende ansvaret for oplysningerne.

25.5.3. *Behandling af og kontrol med transportable databærere*

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

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.

25.5.4. *Afklassificering og destruktion af databærere*

Databærere, der anvendes til lagring af EU-klassificerede oplysninger, kan nedklassificeres eller afklassificeres efter en procedure, der er godkendt af sikkerhedsgodkendelsesmyndigheden.

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

Hvis databærere ikke må afklassificeres eller genbruges, skal de destrueres efter den ovenfor nævnte procedure.

25.5.5. *Kommunikationssikkerhed*

Lederen af Kommissionens Sikkerhedskontor er kryptografisk myndighed.

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.

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 og produkter i forbindelse hermed godkendes specifikt til formålet af sikkerhedsgodkendelsesmyndigheden.

Under videregivelsen skal oplysninger, der er klassificeret EU SECRET eller højere, beskyttes ved hjælp af kryptografiske metoder eller produkter, der er godkendt af det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, efter høring af Kommissionens rådgivende gruppe for sikkerhedspolitik. Under videregivelsen skal oplysninger, der er klassificeret EU CONFIDENTIAL eller EU RESTRICTED, beskyttes ved hjælp af kryptografiske metoder eller produkter, der er godkendt af det medlem af Kommissionens krypteringsmyndighed efter høring af Kommissionens rådgivende gruppe for sikkerhedspolitik.

Detaljerede regler for videregivelse af EU-klassificerede oplysninger fastlægges i specifikke sikkerhedsinstruktioner, der godkendes af Kommissionens Sikkerhedskontor efter høring af Kommissionens rådgivende gruppe for sikkerhedspolitik.

Under ekstraordinære operative forhold kan oplysninger, der er klassificeret EU RESTRICTED, EU CONFIDENTIAL eller EU SECRET, videregives i klar tekst, såfremt der i hvert enkelt tilfælde er givet udtrykkelig bemyndigelse hertil, og det registreres af oplysningernes ejer. 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.

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.

25.5.6. *Installation og strålingssikkerhed*

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 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.

Systemer, der behandler oplysninger, der er klassificeret EU CONFIDENTIAL 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«.

Tempest-modforholdsregler skal revideres og godkendes af Tempest-myndigheden (jf. 25.3.2).

25.6. **Sikkerhed under behandling**

25.6.1. *Sikkerhedsdriftsprocedurer*

Sikkerhedsdriftsprocedurerne definerer de principper, der skal følges i sikkerhedsspørgsmål, de driftsprocedurer, der skal følges, samt medarbejderansvar. Sikkerhedsdriftsprocedurerne udarbejdes under ansvar af det tekniske systems driftsmyndighed.

25.6.2. *Softwarebeskyttelse/konfigurationsstyring*

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.

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

25.6.3. *Kontrol af, om der findes skadelig software/computervirus*

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

Alle databærere, der ankommer til Kommissionen, skal undersøges for skadelig software/computervirus, inden de tilkobles et system.

25.6.4. *Vedligeholdelse*

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 IT-området.

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

25.7. **Anskaffelse af materiel**

25.7.1. *Generelt*

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 en af EU's medlemsstater i henhold til internationale kriterier (som f.eks. de fælles kriterier for sikkerhedsevaluering af informationsteknologi, ref. ISO 15408). Der skal følges nogle særlige procedurer for at opnå ACPC-godkendelse.

Ved beslutningen om, hvorvidt udstyr, specielt databærere, bør leases i stedet for købes, skal det tages i betragtning, dels at udstyr, der en gang har været anvendt til behandling af EU-klassificerede oplysninger, ikke må frigives uden for et passende sikkert miljø uden først at være blevet afklassificeret og godkendt af sikkerhedsgodkendelsesmyndigheden, dels at en sådan godkendelse ikke altid er mulig.

25.7.2. *Godkendelse*

Alle systemer, for hvilke der skal opstilles systemspecifikke sikkerhedskrav forud for behandling af EU-klassificerede oplysninger, godkendes af sikkerhedsgodkendelsesmyndigheden på grundlag af oplysninger i 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 Kommissionen og andre organisationer, skal Kommissionen og relevante sikkerhedsmyndigheder gensidigt være enige om godkendelsen.

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

25.7.3. *Evaluering og certificering*

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.

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

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

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.

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

25.7.4. *Rutinekontrol af sikkerhedsfeatures med henblik på fortsat godkendelse*

Det tekniske systems driftsmyndighed kan fastlægge rutinekontrolprocedurer, som skal sikre, at alle sikkerhedsfeatures i systemet fortsat er gyldige.

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 det tekniske systems 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.

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

25.8. **Midlertidig eller lejlighedsvis anvendelse**

25.8.1. *Sikkerhed for mikrocomputere/personlige computere*

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.

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

25.8.2. *Brug af privatejet IT-udstyr i forbindelse med officielt kommissionsarbejde*

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

Privatejet hardware, software og databærere må ikke bringes ind på noget Klasse I- eller Klasse II-område, hvor der behandles EU-klassificerede oplysninger, uden skriftlig tilladelse fra lederen af Kommissionens Sikkerhedskontor. En sådan tilladelse kan af tekniske årsager kun gives i undtagelsestilfælde.

25.8.3. *Brug af IT-udstyr, der ejes af kontrahent eller er leveret af en medlemsstat, i forbindelse med officielt kommissionsarbejde*

I organisationer, der bidrager til Kommissionens officielle arbejde, kan lederen af Kommissionens Sikkerhedskontor tillade, at der anvendes IT-udstyr og software, som ejes af kontrahenter. Det kan også tillades, at der anvendes IT-udstyr og software, som er leveret af en medlemsstat; i så fald skal IT-udstyret opføres i Kommissionens relevante fortegnelse over udstyr. Hvis IT-udstyret skal anvendes til behandling af EU-klassificerede oplysninger, skal den relevante sikkerhedsgodkendelsesmyndighed høres, således at de elementer af INFOSEC, der gælder for brugen af det pågældende udstyr, tages korrekt i betragtning og gennemføres korrekt.

26. VIDEREGIVELSE AF EU-KLASSIFICEREDE OPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

26.1.1. *Principperne for videregivelse af EU-klassificerede oplysninger*

Kommissionen beslutter som et kollegium, hvorvidt EU-klassificerede oplysninger kan videregives til tredjelande og internationale organisationer, på grundlag af:

— arten og indholdet af sådanne oplysninger

— modtagernes behov for oplysningerne

— EU's interesse i videregivelsen.

Udstederen af de EU-klassificerede oplysninger, der eventuelt skal videregives, bliver bedt om at godkende videregivelsen.

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. Kommissionens rådgivende gruppe for sikkerhedspolitik afgiver teknisk udtalelse til Kommissionen om sådanne spørgsmål.

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 Kommissionens anvisninger.

26.1.2. *Niveauer*

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

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.

Samarbejdsniveauet er afgørende for, hvilke procedurer og sikkerhedsforskrifter der gælder, jf. bilag 3, 4 og 5.

26.1.3. *Sikkerhedsaftaler*

Fastslår Kommissionen, at der er et permanent eller langsigtet behov for udveksling af klassificerede oplysninger mellem Kommissionen og tredjelande eller internationale organisationer, udarbejder den 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.

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 EU RESTRICTED.

Udkast til aftaler om sikkerhedsprocedurer eller aftalememoranda behandles i Kommissionens rådgivende gruppe for sikkerhedspolitik, før de forelægges Kommissionen til afgørelse.

Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål anmoder de nationale sikkerhedsmyndigheder om den nødvendige bistand for at sikre, at de oplysninger, der videregives, anvendes og beskyttes i overensstemmelse med bestemmelserne i aftalerne om sikkerhedsprocedurer eller aftalememorandaene.

Tillæg 1

SAMMENLIGNENDE OVERSIGT OVER DE NATIONALE KLASSIFIKATIONSGRADER

Klassifikationsgrad i EU	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
Klassifikationsgrad i NATO (1)				
Klassifikationsgrad i WEU	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Klassifikationsgrad i Euratom (2)	EURA Top Secret	EURA Secret	EURA Confidential	EURA Restricted
Belgien	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	STRENG GEHEIM	GEHEIM	VS (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grækenland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spanien	Secreto	Reservado	Confidencial	Difusión limitada
Frankrig	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Nederlandene	STG Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Østrig	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sverige	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Det Forenede Kongerige	Top Secret	Secret	Confidential	Restricted

(1) NATO — Sammenhængen med NATO's klassifikationsgrader vil blive fastlagt i forbindelse med forhandlingen om sikkerhedsaftalen mellem Kommissionen og NATO.
(2) Euratom-forordning nr. 3 af 31. juli 1958 om beskyttelse af klassificerede Euratom-oplysninger.
(3) Tyskland: VS = Verschlusssache
(4) Frankrig: klassifikationsgraden »Très Secret Défense« anvendes i forbindelse med statshemmeligheder, ændring kræver bemyndigelse fra premierministeren.

Tillæg 2

PRAKTISK KLASSIFIKATIONSVEJLEDNING

Denne vejledning må ikke opfattes som en ændring af de grundlæggende bestemmelser i afsnit 16, 17, 20 og 21.

Klassifikationsgrad	Hvornår	Hvem	Mærkning	Nedklassificering/afklassificering/destruktion	
				Hvem	Hvornår
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 [16.1].	Ved lækage af oplysninger, der er klassificeret EU TOP SECRET, er der sandsynlighed for: — at stabiliteten i EU, i én af medlemsstaterne eller i venligtsindede lande direkte bringes i fare — at forbindelserne med venligtsindede regeringer direkte skades i overordentlig alvorlig grad — at et stort antal menneskeliv går tabt — at medlemsstaternes eller andre bidragyderes operative effektivitet eller overordentlig vigtige sikkerheds- eller efterretningsoperationers fortsatte effektivitet skades i overordentlig alvorlig grad — at EU's eller medlemsstaternes økonomi påføres alvorlig langvarig skade.	Personer med særlig bemyndigelse (udstederne), generaldirektører, ledere af en tjeneste [17.1] Udstederen skal anføre en dato, en frist eller en begivenhed, efter hvilken indholdet kan nedklassificeres eller afklassificeres. [16.2] I modsat fald skal vedkommende tage klassifikationsgraden op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [17.3].	EU TOP SECRET påføres dokumenter med denne klassifikationsgrad, og, hvor dette er relevant, tilføjes en sikkerhedsangivelse og/eller forsvarspåtegningen ESDP mekanisk eller i hånden [16.4, c), 16.3]. EU-klassifikationsgraden og sikkerhedsangivelser 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 påføres eksemplarnummer, som anbringes på første side sammen med en angivelse af det samlede sideantal. Evt. bilag anføres på første side [21.1].	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [17.3]. Dokumenter, der er klassificeret EUR TOP SECRET, destrueres af det centrale sekretariat eller et undersekretariat med ansvar herfor. Hvert af de destruerede dokumenter anføres i en destruktionsattest, som underskrives af den kontrolansvarlige på EU TOP SECRET-niveau og af den medarbejder, der overværer destruktionen, og som skal være sikkerhedsgodkendt til EU TOP SECRET. Sådanne destruktioner journaliseres. Sekretariatet opbevarer destruktionsattesterne og fordelingslisten i 10 år [22.5].	Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres [22.5]. Dokumenter, der er klassificeret EU TOP SECRET, herunder alt klassificeret affald, der stammer fra forberedelsen af dokumenter, der er klassificeret EU TOP SECRET, som f. eks. beskadigede eksemplarer, arbejdstekster, noter og gennemslagspapir destrueres under opsyn af en kontrolansvarlig, 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 [22.5].

Klassifikationsgrad	Hvornår	Hvem	Mærkning	Nedklassificering/afklassificering/destruktion	
				Hvem	Hvornår
EU SECRET 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 [16.1].	Ved lækage af oplysninger, der er klassificeret EU SECRET, 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.	Bemyndigede personer (udstederne), generaldirektører, ledere af en tjeneste [17.1] Udstederen skal anføre en dato eller frist, efter hvilken indholdet kan nedklassificeres eller afklassificeres. [16.2] I modsat fald skal vedkommende tage klassifikationsgraden op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [17.3].	EU SECRET påføres dokumenter med denne klassifikationsgrad, og, hvor dette er relevant, tilføjes en sikkerhedsangivelse og/eller forsvarspåtegningen ESDP mekanisk eller i hånden [16.4, c), 16.3]. EU-klassifikationsgraden og sikkerhedsangivelser 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 påføres eksemplarnummer, som anbringes på første side sammen med en angivelse af det samlede sideantal. Evt. bilag anføres på første side [21.1].	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [17.3]. Dokumenter, der er klassificeret EU SECRET, destrueres af det sekretariat, der er ansvarligt for disse dokumenter, under tilsyn af en sikkerhedsgodkendt person. Dokumenter, der er klassificeret EU SECRET, og som destrueres, opføres på underskrevne destruktionsattester, der opbevares af sekretariatet i mindst tre år tillige med fordelingslisten [22.5].	Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres [22.5]. Dokumenter, der er klassificeret EU SECRET, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og gennemslagspapir, destrueres ved afbrænding, opløsning, makulering eller på anden måde reducering til et produkt, der hverken kan genkendes eller rekonstrueres [22.5].

Klassifikationsgrad	Hvornår	Hvem	Mærkning	Nedklassificering/afklassificering/destruktion	
				Hvem	Hvornår
EU-CONFIDENTIAL 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 [16.1].	Ved lækage af oplysninger, der er klassificeret EU CONFIDENTIAL, er der sandsynlighed for: — at de diplomatiske forbindelser vil lide materiel skade, dvs. at det vil medføre formelle protester eller andre sanktioner — at den individuelle sikkerhed eller frihed vil tage skade — 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 levedygtighed i væsentlig grad — at det vil vanskeliggøre efterforskningen af eller gøre det lettere at begå alvorlig kriminalitet — at det i væsentlig grad vil stride mod EU's eller medlemsstaternes finansielle, monetære, økonomiske og kommercielle interesser — at det i væsentligt omfang vil vanskeliggøre udviklingen eller gennemførelsen af EU-politikker — at vigtige EU-aktiviteter afsluttes eller på anden måde forstyrres i væsentlig grad.	Bemyndigede personer (udstederne), generaldirektører, ledere af en tjeneste [17.1] 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 [17.3].	EU CONFIDENTIAL påføres dokumenter med denne klassifikationsgrad og, hvor det er relevant, tilføjes en sikkerhedsangivelse og/eller forsvarspåtegningen ESDP mekanisk eller i hånden eller ved kopiering på fortrykt registreret papir [16.4, c), 16.3]. EU-klassifikationsgraden 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 [21.1].	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [17.3]. Dokumenter, der er klassificeret EU CONFIDENTIAL, destrueres af det sekretariat, der er ansvarligt for disse dokumenter, under tilsyn af en sikkerhedsgodkendt person. Destruktionen registreres i overensstemmelse med nationale bestemmelser eller, hvis det drejer sig om Kommissionen eller decentrale EU-organer, efter instrukser fra formanden [22.5].	Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres [22.5]. Dokumenter, der er klassificeret EU CONFIDENTIAL, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og gennemslagspapir, destrueres ved afbrænding, opløsning, makulering eller på anden måde reducering til et produkt, der hverken kan genkendes eller rekonstrueres [22.5].

Klassifikationsgrad	Hvornår	Hvem	Mærkning	Nedklassificering/afklassificering/destruktion	
				Hvem	Hvornår
EU RESTRICTED 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 [16.1].	Ved lækage af oplysninger, der er klassificeret EU RESTRICTED, 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 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.	Bemyndigede personer (udstederne), generaldirektører, ledere af en tjeneste [17.1] Udstederen skal anføre en dato, en frist eller en begivenhed, efter hvilken indholdet kan nedklassificeres eller afklassificeres [16.2]. I modsat fald skal vedkommende tage klassifikationsgraden op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig [17.3].	EU RESTRICTED påføres dokumenter med denne klassifikationsgrad og, hvor det er relevant, tilføjes en sikkerhedsangivelse og/eller forsvarspåtegningen ESDP mekanisk ellenr.r elektronisk [16.4, c), 16.3]. EU-klassifikationsgraden og sikkerhedsangivelser anføres øverst på den første side, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato [21.1].	Afklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf [17.3]. Dokumenter, der er klassificeret EU RESTRICTED destrueres af det sekretariat, der er ansvarligt for dokumentet, i overensstemmelse med formandens instruktioner [22.5].	Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres [22.5].

Tillæg 3

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande og internationale organisationer: niveau 1-samarbejde

PROCEDURER

1. Kompetencen til at videregive EU-klassificerede oplysninger til lande, der ikke er medlemmer af Den Europæiske Union, eller til internationale organisationer, hvis sikkerhedspolitik og -bestemmelser svarer til EU's, tilkommer Kommissionen som kollegium.

2. Indtil der vedtages en sikkerhedsaftale, er det det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, som behandler anmodninger om videregivelse af EU-klassificerede oplysninger.

3. I forbindelse hermed skal han/hun:

   — indhente en udtalelse fra udstederen af de EU-klassificerede oplysninger, der ønskes videregivet

   — tage 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

   — indhente en udtalelse fra Kommissionens rådgivende gruppe for sikkerhedspolitik om, hvorvidt der kan fæstes lid til de anmodende stater eller internationale organisationer.

4. Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål fremsender anmodningen og udtalelsen fra Kommissionens rådgivende gruppe for sikkerhedspolitik til Kommissionen til afgørelse.

DE SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

5. Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål meddeler de anmodende stater eller internationale organisationer, hvorvidt Kommissionen har besluttet at tillade videregivelsen af EU-klassificerede oplysninger.

6. 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 EU CONFIDENTIAL 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.

8. Fremsendelse af dokumenter

   a) Den praktiske fremsendelse af dokumenter foregår efter aftale. Indtil en sådan aftale er truffet, anvendes bestemmelserne i afsnit 21. I aftalen skal bl. a. angives, hvilket sekretariat EU-klassificerede oplysninger skal fremsendes til.

   b) Hvis de klassificerede oplysninger, som Kommissionen har givet bemyndigelse til at videregive, omfatter oplysninger, der er klassificeret EU TOP SECRET, skal den modtagende stat eller internationale organisation oprette et centralt EU-sekretariat og om nødvendigt EU-undersekretariater. Disse sekretariater skal overholde bestemmelser, der nøje svarer til bestemmelserne i afsnit 22, i disse sikkerhedsforskrifter.

9. Registrering

   Så snart et sekretariat modtager et EU-dokument, der er klassificeret EU CONFIDENTIAL 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 22, i disse sikkerhedsforskrifter. Kopi af destruktionsattesten for dokumenter, der er klassificeret EU SECRET eller 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, udfærdiges oversættelser eller tages uddrag af dokumenter, der er klassificeret EU CONFIDENTIAL eller EU SECRET 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 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 Kommissionens 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) Kommissionens 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 Kommissionens Sikkerhedskontor med henblik på at forebygge gentagelser, gennemføres.

14. Inspektion

Kommissionens 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.

15. Rapportering

Medmindre der er indgået en sikkerhedsaftale, skal en stat eller international organisation, så længe 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.

Tillæg 4

Retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande og 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 den, der har udstedt oplysningerne. Det er Kommissionen som kollegium, der har beføjelse til at videregive EU-klassificerede oplysninger udarbejdet i Kommissionen.

2. Denne beføjelse er i princippet begrænset til oplysninger, der højst er klassificeret EU SECRET eller lavere; den omfatter ikke klassificerede oplysninger, der er beskyttet af særlige sikkerhedsangivelser eller mærker.

3. Indtil der vedtages en sikkerhedsaftale, er det det medlem af Kommissionen, der har ansvaret for sikkerhedsspørgsmål, som behandler anmodninger om videregivelse af EU-klassificerede oplysninger.

4. I forbindelse hermed skal han/hun:
   — indhente en udtalelse fra udstederen af de EU-klassificerede oplysninger, der ønskes videregivet
   — tage de nødvendige kontakter 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
   — indkalde til møde i Kommissionens rådgivende gruppe for sikkerhedspolitik eller, om nødvendigt efter en stiltiende samtykkeprocedure, rette henvendelse til medlemsstaternes nationale sikkerhedsmyndigheder med henblik på at indhente en udtalelse fra Kommissionens rådgivende gruppe for sikkerhedspolitik

5. Udtalelsen fra Kommissionens rådgivende gruppe for sikkerhedspolitik skal omfatte følgende:
   — en vurdering af 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.)
   — en vurdering af, hvorvidt udstederen bør nedklassificere eller afklassificere oplysningerne, inden de videregives til de pågældende lande eller internationale organisationer.

6. Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål fremsender anmodningen og udtalelsen fra Kommissionens rådgivende gruppe for sikkerhedspolitik til Kommissionen til afgørelse.

SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

7. Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål meddeler de anmodende stater eller internationale organisationer, hvorvidt Kommissionen har besluttet at tillade videregivelsen af EU-klassificerede oplysninger, og om der er nogen restriktioner.

8. 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 de af Kommissionen fastsatte bestemmelser

9. Nedenstående beskyttelsesregler anvendes, medmindre Kommissionen efter at have indhentet teknisk udtalelse fra Kommissionens rådgivende gruppe for sikkerhedspolitik, beslutter at anvende en særlig procedure for behandling af EU-klassificerede dokumenter (fjerne EU-klassifikationsangivelsen, særlig påtegning eller lign.).

10. 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 klassificerede oplysninger, der er videregivet af Kommissionen, skal være i besiddelse af en national sikkerhedsgodkendelse eller adgangsbemyndigelse på det relevante niveau svarende til niveauet i EU, jf. den sammenlignende oversigt.

    c) De nationale sikkerhedsgodkendelser eller adgangsbemyndigelser fremsendes til orientering til formanden.

11. Fremsendelse af dokumenter

Den praktiske fremsendelse af dokumenter foregår efter aftale. Indtil en sådan aftale er truffet, anvendes bestemmelserne i afsnit. I aftalen skal bl.a. angives, hvilket sekretariat EU-klassificerede oplysninger skal sendes til, den nøjagtige adresse, som dokumenterne skal sendes til, samt de kurer- eller posttjenester, der skal anvendes til fremsendelse af de EU-klassificerede oplysninger.

12. Registrering ved modtagelse

Den modtagende stats nationale sikkerhedsmyndighed eller tilsvarende organ i den stat, der på sine myndigheders vegne modtager de klassificerede oplysninger fremsendt af Kommissionen, eller den modtagende internationale organisations sikkerhedskontor skal oprette et særligt register 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.

13. Returnering af dokumenter

Når en modtager returnerer et klassificeret dokument til Kommissionen, skal det ske som anført i afsnittet om fremsendelse af dokumenter ovenfor.

14. Beskyttelse

a) Når dokumenterne ikke er i brug, skal de opbevares i sikre bokse og skabe, 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 de sikre bokse og skabe 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 sikre bokse og skabe, 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 EU CONFIDENTIAL eller højere, eller tages uddrag af det uden bemyndigelse fra Kommissionens Sikkerhedskontor.

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

15. Fysisk sikkerhed

a) Sikre bokse og skabe til opbevaring af EU-klassificerede dokumenter skal altid være aflåst.

b) Når vedligeholdelses- og rengøringspersonale skal have adgang til eller arbejde i et rum, hvor sådanne sikre bokse og skabe 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 normal arbejdstid (om natten, i weekender og på officielle fridage) skal sikre bokse og skabe, der indeholder EU-klassificerede dokumenter, være beskyttet enten af en vagt eller af et automatisk alarmsystem.

16. 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 Kommissionens Sikkerhedskontor eller den nationale sikkerhedsmyndighed i den medlemsstat, som har taget initiativ til at fremsende dokumenterne (med kopi til Kommissionens Sikkerhedskontor)

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

17. Inspektion

Kommissionens 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.

18. Rapportering

Medmindre der er indgået en sikkerhedsaftale, skal en stat eller international organisation, så længe 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.

Tillæg 5:

retningslinjer for videregivelse af EU-klassificerede oplysninger til tredjelande og internationale organisationer: niveau 3-samarbejde

PROCEDURER

1. Under visse særlige omstændigheder kan Kommissionen undertiden 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.

2. Kompetencen til at videregive EU-klassificerede oplysninger til tredjelande eller til internationale organisationer, hvis sikkerhedspolitik og -bestemmelser afviger markant fra EU's, tilkommer den, der har udstedt oplysningerne. Det er Kommissionen som kollegium, der har beføjelse til at videregive EU-klassificerede oplysninger udarbejdet i Kommissionen.

   Det er i princippet begrænset til oplysninger, der er klassificeret EU SECRET eller lavere; klassificerede oplysninger, der er beskyttet af særlige sikkerhedsangivelser eller mærker, er udelukket.

3. Kommissionen 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.

4. Hvis Kommissionen er indforstået, skal medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål:
   — indhente en udtalelse fra udstederen af de EU-klassificerede oplysninger, der ønskes videregivet
   — indkalde til møde i Kommissionens rådgivende gruppe for sikkerhedspolitik eller, om nødvendigt efter en stiltiende samtykkeprocedure, rette henvendelse til medlemsstaternes nationale sikkerhedsmyndigheder med henblik på at indhente en udtalelse fra Kommissionens rådgivende gruppe for sikkerhedspolitik.

5. Udtalelsen fra Kommissionens rådgivende gruppe for sikkerhedspolitik skal omfatte følgende:

   a) en vurdering af sikkerhedsrisikoen for EU eller dens medlemsstater

   b) klassifikationsgraden af de oplysninger, der kan videregives

   c) nedklassificering eller afklassificering før videregivelsen af oplysningerne

   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.).

6. 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. Kommissionens rådgivende gruppe for sikkerhedspolitik kan henstille, at der:
   — benyttes en særlig påtegning eller kodebetegnelse
   — benyttes et særligt klassifikationssystem, der kæder oplysningernes følsomhed sammen med de kontrolforanstaltninger, der kræves af modtageren i forbindelse med fremsendelse af dokumenterne.

7. Formanden fremsender udtalelsen fra Kommissionens rådgivende gruppe for sikkerhedspolitik til Kommissionen til afgørelse.

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

9. Medlemmet af Kommissionen med ansvar for sikkerhedspørgsmål informerer medlemsstaterne om oplysningernes art og klassifikationsgrad og om, hvilke organisationer og lande oplysningerne kan videregives til ifølge Kommissionens beslutning.

10. Kommissionens Sikkerhedskontor træffer alle de nødvendige foranstaltninger til at lette en eventuel senere skadesvurdering og gennemgang af procedurerne.

    I fald vilkårene for samarbejdet ændres, tager Kommissionen beslutningen op til fornyet overvejelse.

DE SIKKERHEDSFORANSTALTNINGER, MODTAGERNE SKAL TRÆFFE

11. Medlemmet af Kommissionen med ansvar for sikkerhedsspørgsmål meddeler de anmodende stater eller internationale organisationer, hvorvidt Kommissionen har besluttet at tillade videregivelsen af EU-klassificerede oplysninger, og hvilke detaljerede beskyttelsesbestemmelser Kommissionen har vedtaget efter forslag fra Kommissionens rådgivende gruppe for sikkerhedspolitik.

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

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

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

13. Fremsendelse af dokumenter

a) De praktiske procedurer for fremsendelse af dokumenter fastsættes ved aftale mellem Kommissionens 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 EU CONFIDENTIAL 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.

14. Registrering ved modtagelse

Den modtagende stats nationale sikkerhedsmyndighed eller tilsvarende organ i den stat, der på sine myndigheders vegne modtager de klassificerede oplysninger fremsendt af Kommissionen, eller den modtagende internationale organisations sikkerhedskontor skal oprette et særligt register 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.

15. Benyttelse og beskyttelse af de udvekslede klassificerede oplysninger

a) Oplysninger, der er klassificeret EU SECRET, skal behandles af særligt udpegede medarbejdere, der er bemyndiget til at få adgang til oplysninger med denne klassifikationsgrad. Oplysningerne skal opbevares i sikre bokse og skabe 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 sikre bokse og 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 EU SECRET, fremsendes med diplomatpost, sikret postforsendelse eller sikrede telekommunikationssystemer. De må kun kopieres med udstederens skriftlige samtykke. Alle eksemplarer skal registreres og overvåges. Der skal udstedes modtagelsesbevis for alle transaktioner i forbindelse med sådanne dokumenter.

b) Oplysninger, der er klassificeret EU CONFIDENTIAL, skal behandles af særligt udpegede tjenestemænd, der er bemyndiget til at blive informeret om emnet. Dokumenter skal opbevares i aflåste sikre bokse og skabe i kontrollerede områder.

Oplysninger, der er klassificeret EU CONFIDENTIAL, 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 EU RESTRICTED, skal behandles i lokaler, hvortil der ikke er adgang for personer uden bemyndigelse, og skal opbevares i aflåste sikre bokse og skabe. 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.

16. Destruktion

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

17. Brud på sikkerhedsbestemmelserne

Ved lækage af oplysninger, der er klassificeret EU CONFIDENTIAL eller EU SECRET, eller der er mistanke om en sådan lækage, skal den pågældende stats nationale sikkerhedsmyndighed eller den pågældende organisations sikkerhedschef gennemføre en undersøgelse af omstændighederne. Kommissionens sikkerhedskontor skal underrettes om resultatet af denne undersøgelse. Der skal træffes de nødvendige foranstaltninger til at afhjælpe mangelfulde procedurer eller opbevaringsmetoder, hvis de er årsagen til lækagen af oplysningerne.

Tillæg 6

FORTEGNELSE OVER FORKORTELSER

ACPC	Rådgivende Udvalg for Indkøb og Aftaler
CrA	Krypteringsmyndighed
CISO	Central edb-sikkerhedsansvarlig
COMPUSEC	Edb-sikkerhed
COMSEC	Kommunikationssikkerhed
CSO	Kommissionens Sikkerhedskontor
ESDP	Fælles europæisk sikkerheds- og forsvarspolitik
EUCI	EU-klassificerede oplysninger
IA	INFOSEC-myndighed
INFOSEC	Informationssikkerhed
IO	Ejer af oplysninger
ISO	Den Internationale Standardiseringsorganisation
IT	Informationsteknologi
LISO	Lokal edb-sikkerhedsansvarlig
LSO	Lokal sikkerhedsansvarlig
MSO	Sikkerhedsansvarlig for møder
NSA	National sikkerhedsmyndighed
PC	Personlig computer
RCO	Sekretariatskontrolansvarlig
SAA	Sikkerhedsgodkendelsesmyndighed
SecOPS	Sikkerhedsdriftsprocedurer
SSRS	Specifikke sikkerhedskrav
TA	Tempest-myndighed
TSO	Tekniske systems driftsmyndighed